

**THE DEPARTMENT OF HOMELAND SECURITY  
STATE AND LOCAL FUSION CENTER PROGRAM:**

---

**HEARING**

BEFORE THE

**SUBCOMMITTEE ON INTELLIGENCE,  
INFORMATION SHARING, AND  
TERRORISM RISK ASSESSMENT**

OF THE

**COMMITTEE ON HOMELAND SECURITY  
HOUSE OF REPRESENTATIVES**

**ONE HUNDRED TENTH CONGRESS**

**FIRST SESSION**

**MARCH 14, 2007**

**Serial No. 110-15**

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpoaccess.gov/congress/index.html>

U.S. GOVERNMENT PRINTING OFFICE

35-274 PDF

WASHINGTON : 2009

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

## COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,	PETER T. KING, New York
EDWARD J. MARKEY, Massachusetts	LAMAR SMITH, Texas
NORMAN D. DICKS, Washington	CHRISTOPHER SHAYS, Connecticut
JANE HARMAN, California	MARK E. SOUDER, Indiana
PETER A. DeFAZIO, Oregon	TOM DAVIS, Virginia
NITA M. LOWEY, New York	DANIEL E. LUNGREN, California
ELEANOR HOLMES NORTON, District of Columbia	MIKE ROGERS, Alabama
ZOE LOFGREN, California	BOBBY JINDAL, Louisiana
SHEILA JACKSON LEE, Texas	DAVID G. REICHERT, Washington
DONNA M. CHRISTENSEN, U.S. Virgin Islands	MICHAEL T. McCAUL, Texas
BOB ETHERIDGE, North Carolina	CHARLES W. DENT, Pennsylvania
JAMES R. LANGEVIN, Rhode Island	GINNY BROWN-WAITE, Florida
HENRY CUELLAR, Texas	MARSHA BLACKBURN, Tennessee
CHRISTOPHER P. CARNEY, Pennsylvania	GUS M. BILIRAKIS, Florida
YVETTE D. CLARKE, New York	DAVID DAVIS, Tennessee
AL GREEN, Texas	
ED PERLMUTTER, Colorado	
VACANCY	

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*

TODD GEE, *Chief Counsel*

MICHAEL TWINCHEK, *Chief Clerk*

ROBERT O'CONNOR, *Minority Staff Director*

---

## SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

NORMAN D. DICKS, Washington	DAVID G. REICHERT, Washington
JAMES R. LANGEVIN, Rhode Island	CHRISTOPHER SHAYS, Connecticut
CHRISTOPHER P. CARNEY, Pennsylvania	CHARLES W. DENT, Pennsylvania
ED PERLMUTTER, Colorado	PETER T. KING, New York ( <i>Ex Officio</i> )
BENNIE G. THOMPSON, Mississippi ( <i>Ex Officio</i> )	

THOMAS M. FINAN, *Director and Counsel*

BRANDON DECLET, *Counsel*

NATALIE NIXON, *Deputy Chief Clerk*

DERON MCELROY, *Minority Senior Professional Staff Member*

(II)

# CONTENTS

	Page
STATEMENTS	
The Honorable Jane Harman, a Representative in Congress from the State of California, and Chair, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment:	
Oral Statement .....	1
Prepared Statement .....	3
The Honorable David G. Reichert, a Representative in Congress from the State of Washington, and Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment .....	14
The Honorable Charles W. Dent, a Representative in Congress from the State of Pennsylvania .....	18
The Honorable Norman D. Dicks, a Representative in Congress from the State of Washington .....	16
WITNESSES	
PANEL I	
Mr. Charles E. Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, Department of Homeland Security:	
Oral Statement .....	5
Prepared Statement .....	8
Mr. Daniel W. Sutherland, Officer for Civil Rights and Civil Liberties, Department of Homeland Security:	
Oral Statement .....	20
Prepared Statement .....	21
Mr. Hugo Tuefel, Privacy Officer, Department of Homeland Security:	
Oral Statement .....	24
Prepared Statement .....	25
FOR THE RECORD	
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi:	
Prepared Statement .....	31
Questions and Responses:	
Responses from Mr. Daniel W. Sutherland and Mr. Hugo Tuefel .....	32



## ADVANCING INFORMATION SHARING WHILE SAFEGUARDING CIVIL LIBERTIES

---

Wednesday, March 14, 2007

U.S. HOUSE OF REPRESENTATIVES,  
COMMITTEE ON HOMELAND SECURITY,  
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION  
SHARING, AND TERRORISM RISK ASSESSMENT,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 3:40 p.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chairwoman of the subcommittee] presiding.

Present: Representatives Harman, Dicks, Reichert, and Dent.

Ms. HARMAN. Good afternoon. The subcommittee will come to order. The subcommittee is meeting today to receive testimony on State and local fusion centers and on advancing information sharing while safeguarding civil liberties.

Earlier this week, I led a member tour to two facilities in the D.C. area with critical Homeland Security missions—the National Counterterrorism Center and the Maryland Coordination and Analysis Center, or MCAC, in suburban Baltimore. I, frankly, saw some things that were inspirational and a few things that worried me. Representatives Perlmutter, Shays, Wolf, and I were particularly impressed by the NCTC, the Nation's fusion center for all terrorism-related information. It is clear that the NCTC has played a key role in improving information sharing across the Federal Government, and Admiral Scott Redd and his team are to be commended for their work there.

I was disturbed, however, by what I learned about the emerging plans for the Interagency Threat Assessment and Coordination Group, or the ITACG, that our witness, Mr. Allen described in his testimony here last month. How this group, which is supposed to be creating unclassified products for State, local and tribal law enforcement officers across the country is going to be effective with only one local law enforcement person on staff is beyond me, and I am a bit disappointed that DHS, the agency that is supposed to be advocating for State and locals, has not fought harder to expand the number of nonFederal players at the ITACG table.

The subcommittee may have to take a very close look at the ITACG in the current months, in the coming months, and I am certain that chairman would agree with me. It also is a good thing that to my right sits a former sheriff who I think would have some insights into the value of local participation at the Federal level and creating the products that are then distributed for local consumption.

(1)

Our group also paid a visit to the Maryland Coordination and Analysis Center, the MCAC, in West Baltimore, as I mentioned. While the MCAC staffers were enthusiastic about their work and impressive, it is clear that the organization has no budget and is staffed mainly by detailees on loan from other agencies. They saw that as a positive because that meant that no one agency was in charge, which they felt would discourage other agencies from participating, but I saw that as a negative because, if any of those agencies faced budget squeezes, the easiest place to squeeze is to remove the detailee from the MCAC, and then there would be that enormous loss of competence. Although the MCAC is turning out impressive intelligence products on a daily basis, the facilities it occupies are, to say the least, modest. I was pleased to meet DHS' staffer, Charlie Allen's person, at the MCAC.

But I left the MCAC with one main conclusion, and that is that all the DHS staff assistance in the world will not get the job done if fusion centers do not have adequate and sustained funding. Without money, they are going to disappear, and the DHS State and Local Fusion Center Program will not succeed.

In addition to sustained funding, we need to institutionalize how we are doing intelligence at these facilities. That means that we should be encouraging not only intelligence fusion but also—and I know our witness agrees—rigorous adoption of privacy and civil liberties' protections as part of the process. I often say that security and liberty are not a zero sum exercise.

It is not that you get more of one and less of the other; it is that you get more of both or less of both, and so it is absolutely critical that we factor both in at the front end, and then we give confidence to those whose information we hope will be contributed to these fusion centers and whose information may be the critical piece that helps us unravel a plot before it is launched against America and American interests. Of course, we are pleased that Charlie Allen is back to address these concerns.

Let me say, Charlie, that I have been through the President's requested budget numbers, and I, frankly, do not see how you can meet your goal of having your staff in up to 40 fusion centers by the end of fiscal year 2008 without some very creative thinking and reprioritization on your part or without some additional help on our part. While we can not get into any classified figures and staffing levels here, I hope you will be able to shed light on where the President's budget request leaves you and on how you will go about meeting your fusion center targets, given the budget constraints you are facing.

We also hope to hear more about the privacy and civil liberties education that you have mentioned in recent months before this subcommittee and before the Senate Select Committee on Intelligence.

In that regard, I am pleased that we have with us today both the Department's Privacy Officer, Hugo Teufel, and its Civil Rights and Civil Liberties Officer, Daniel Sutherland.

I note that this hearing comes on the heels of the National Fusion Center Conference in Florida last week where DHS, DOJ and the DNI and many State and local representatives and some of our staff got together to discuss the very issues on our agenda. I am

happy that we all seem to be on the same page. Now it is time to move to the next chapter.

Welcome again to you.

PREPARED STATEMENT OF HON. JANE HARMAN

Earlier this week, I led a Member tour to two facilities in the DC area with critical homeland security missions—the National Counterterrorism Center and the Maryland Coordination and Analysis Center (MCAC) in suburban Baltimore.

I frankly saw some things that were inspirational and some things that worried me tremendously.

Representatives Perlmutter, Shays, Wolf, and I were particularly impressed by the NCTC, the nation's "fusion center" for all terrorism-related information. It's clear that that the NCTC has played a key role in improving information sharing across the Federal government, and Admiral Redd and his team are to be commended for their work there.

I was disturbed, however, by what I learned about the emerging plans for the Interagency Threat Assessment and Coordination Group—the ITACG—that Mr. Allen described in his testimony here last month.

How this group—which is supposed to be creating unclassified products for State, local, and tribal law enforcement officers across the country—is going to be effective with ONLY ONE local law enforcement person on staff is beyond me.

And I'm disappointed that DHS—the agency that is supposed to be advocating for State and locals—has not fought harder to expand the number of non-Federal players at the ITACG table.

The Subcommittee may have to take a very close look at the ITACG in the coming months, and I am certain the Chairman would agree with me.

We also paid a visit to the Maryland Coordination and Analysis Center (MCAC)—Maryland's State fusion center.

While the MCAC staffers were enthusiastic about their work and are undoubtedly working very hard, it's clear that the organization has no budget and is staffed mainly by detailees on loan from other agencies.

And although the MCAC is turning out impressive intelligence products on a daily basis, the facilities it occupies are—to say the least—very modest.

I was pleased to meet DHS' staffer at the MCAC, but I left the MCAC with one main conclusion: all the DHS staffing in the world won't make a bit of difference if fusion centers do not have adequate and sustained funding.

Without money, they're going to disappear, and DHS' State and Local Fusion Center Program won't make a bit of difference.

In addition to sustained funding, we need to institutionalize how we are doing intelligence at these facilities.

That means that we should be encouraging not only intelligence fusion but also rigorous adoption of privacy and civil liberties protections as part of that process.

We're pleased that Charlie Allen is back to address these concerns.

I've been through the President's requested budget numbers, Charlie, and I frankly don't see how you can meet your goal of having your staff in up to 40 fusion centers by the end of Fiscal Year 2008 without some very creative thinking and re-prioritization on your part.

While we can't get into any classified figures and staffing levels here, I hope you'll be able to shed some light on where the President's budget request leaves you, and how you will go about meeting your fusion center targets given the budget constraints you're facing.

I also want to hear more about the privacy and civil liberties education that you have mentioned in recent months before this Subcommittee and the Senate Select Committee on Intelligence.

In that regard, I'm pleased that we have with us today both the Department's Privacy Officer, Hugo Teufel (pronounced "Too-fell"), and its Civil Rights and Civil Liberties Officer, Mr. Daniel Sutherland.

I note that this hearing comes on the heels of the National Fusion Center Conference in Florida last week—where DHS, DOJ, the DNI, and many State and local representatives got together to discuss the very issues on our agenda today.

I am happy that we all seem to be on the same page. Now it's time to move to the next chapter—specifically, to ensure that the funding and privacy and civil liberties "know how" that is necessary for fusion centers is authorized, appropriated, and put into action while safeguarding civil rights and civil liberties at the same time.

Welcome again to you all.

MS. HARMAN. I will now recognize Sheriff Reichert, the ranking member of the subcommittee, for an opening statement.

Mr. REICHERT. Thank you, Madam Chair.

I want to thank you for holding this important hearing. We are, I think, going to make a great team, and I am glad to see my good friend from Washington State, Norm, here with us today, so the three of us will get to inquire a little bit further after your testimony.

Charlie, it is good to see you again, and I have only met you a few times, but I feel very comfortable with you, and it seems like we have known each other for quite a long time. You are very responsive and always available for questions and guidance, and we all appreciate that on this subcommittee. You know, the process is a little—it always kind of amuses me that politicians speak for a while and those are things, you know, that we need to get on the record, but we also want to hear from the witness, so I will ask you to indulge me just a little bit here while I take the opportunity to express some of my views for the record, and then we will get to the questioning.

You know, I am a sheriff and a law enforcement officer at heart, and there are certain things that touch all of us. Now, as we look ahead to the future of this country and to the gathering of intelligence, the protection of private rights really is at the top of the list. For 33 years, that is what I did was protect people, protect communities, protect neighbors, and protect their rights. A substantial part of the intelligent portion of the authorization bill that we are talking about today will focus on the Department of Homeland Security's involvement in State and local fusion centers. DHS, the FBI and other Federal agencies are participating with local law enforcement in these fusion centers, and many questions are raised as local and Federal agencies partner, including: What role does the Federal Government have? Should there be more money allocated for the Federal role in these centers? Should personnel costs of local law enforcement be funded by the Federal Government since they are now participating in a so-called "nontraditional" law enforcement role?

As a former sheriff of a major county, I was required to reallocate personnel to participate in the joint analytical centers and the JTTS. In knowing the burden this places on local law enforcement, I believe the Federal Government has an obligation to partner with local authorities in the operation and funding of local fusion centers. I look forward to hearing from Mr. Allen on these issues today.

Another pressing issue on many of our minds is civil rights and civil liberties, as I said, and is the main subject of our second panel. It is essential that we have the tools and the resources necessary to protect our Nation from future terrorist attacks. However, DHS and other agencies must have a healthy respect for privacy and other civil rights and civil liberties. We all hear complaints about potential violations in the newspapers, and some of these are real and concerning; some are speculative and lack supporting evidence, but what is important is the establishment of proper training methods and procedures for protecting privacy and civil liberties so that mistakes and abuses can be avoided, detected and



corrected. In this respect, we must recognize the hard and often thankless work of the DHS Privacy Office and the DHS Civil Rights and Civil Liberties Office. Their sole mission is to minimize the Department's impact on people's privacy and rights.

The DHS fusion center work has progressed over the last year on many fronts—from conceptual development, to deploying personnel, to the fusion centers. As part of this development, the Department issued fusion center guidelines and disseminated a fusion center grant planning tool. In the guidelines, DHS specifically focuses on privacy as a minimum consideration for interagency Memorandums of Understanding. DHS also adds as a key element of the guidelines adhering to privacy and civil liberty policies.

As part of the fusion center planning tool, grant funding is allowed to establish a fusion center's critical baseline operations standards. One of these critical baseline standards is the identification and implementation of privacy and civil liberty protections. Every fusion center official that I have spoken with has acknowledged the importance of safeguarding civil liberties. I look forward to hearing from the Department of Homeland Security on what additional work is to be done to follow up with the fusion centers on these important priorities and in ensuring that employees receive appropriate training in privacy and civil liberty issues.

Most recently, I visited the LA Fusion Center and had also visited Seattle's once again—as I am quite familiar with their joint analytical center—as they progress and move toward a fusion center, two very outstanding operations, and DHS' role in both of those fusion centers has been greatly appreciated.

Madam Chair, I yield.

Ms. HARMAN. I thank you for your comments, and I would note that other members of the subcommittee under our committee rules are encouraged to submit opening statements for the record, but we will now proceed directly to our first witness, Charlie Allen, who has been introduced numerous times by this committee and subcommittee, and so I just would point out he is the Department of Homeland Security's Chief Intelligence Officer with a long and distinguished background and a long and distinguished future.

Please summarize your remarks, Mr. Allen, for the record, and we will go directly to questions.

We will have a second panel today to discuss some of the issues that have been raised in the opening statements.

**STATEMENT OF CHARLES E. ALLEN, CHIEF INTELLIGENCE OFFICER, OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY**

Mr. ALLEN. Thank you very much, Chairwoman, Harman, Ranking Member Reichert and Congressman Dicks.

I really do welcome the opportunity to speak about our State and Local Fusion Center Program, and also how we work to protect civil rights and civil liberties. Also, it is a pleasure to be here to know that we have Mr. Hugo Teufel and Dan Sutherland. I appeared with Mr. Sutherland this morning over on the Senate Homeland Security Committee to talk about radicalization. I probably will omit comments about radicalization in my summary here, but I certainly can answer questions on that.

I do want to speak to the Interagency Threat Assessment and Coordination Group, which, by the way, is now called the Federal Coordinating Group. We are beginning to move staff officers who form a core advance team into our location out at Liberty Crossing, as you indicated, and we are beginning to work with Federal and nonFederal partners to staff fully the group. It will be a real opportunity to have sustained, coordinated information sharing down at State and local levels, and we are working to include additional people from State and local governments.

In fact, in the initial stand-up staff, I envision two or three officers, certainly. I do not know exactly what was said out at the NCTC, but we are still working to put together a concept of operations, and I want to assure you that there is going to be growth in State and local government representation.

Let me touch on how the State and Local Fusion Center Program promotes information sharing, and it does this both horizontally between centers across the country and, of course, vertically between the Intelligence Community and the centers while working to safeguard civil liberties and privacy. Protecting privacy and civil liberties remains one of my top organizational priorities. I hold my office to the highest standards in these areas, and we reinforce these principles with all of our employees.

In terms of incorporating privacy and civil liberties training into our fusion center program, the Department of Justice has made strong efforts to establish and provide important training and outreach programs to fusion center personnel. The Global Justice Fusion Center Guidelines, published by the Department of Justice, DHS and in participation with State and local governments, requires fusion centers to create policies that safeguard civil liberties. The National Fusion Center Conference last week, which you alluded to, brought subject matter experts from across the United States to discuss privacy and civil liberties, and there were two sessions, two breakout sessions, devoted to that that were well attended—I was very pleased to see that—and over 600 people came to that conference.

In addition, Federal Intelligence Officers assigned to the fusion centers have to comply with policy obligations regarding annual training requirements for protecting U.S. persons and are abiding by privacy guidelines of the information sharing environment, which, of course, you are well aware of and is managed by Ambassador Ted McNamara. We are working closely with various DHS and the external Civil Liberties and Privacy Office to ensure adequate oversight in these areas and to identify where additional training is needed.

The last time I appeared before this subcommittee, you shared three priorities—information sharing with first presenters, the potential radicalization and reducing overclassification of intelligence. Let me just talk about information sharing with first presenters.

The new DNI, Mike McConnell, recently set forth his vision for the Intelligence Community. He says we all have “a responsibility to provide,” not just to share. When I spoke to you last, I pledged that DHS intelligence would set the standard in this area. Our fusion center program underscores the importance I place in this

area. To this end, the Department created a State and Local Fusion Center Program almost 9 months ago.

This program, as you know, embeds DHS officers into fusion centers to share information, to collaborate on analysis and to identify information of intelligence value at a State and local level, and I believe, on issues of radicalization and also on all threats, there is a lot of information at that level as Ranking Member Reichert pointed out. My officers continue to work with the intelligence officers of DHS operating components and with the Intelligence Community to move tailored and timely intelligence out to the fusion centers. The result is better reporting and validating of actionable information both to our State and local partners and to the Intelligence Community. Our efforts to deploy intelligence analysts to the fusion centers around the country are progressing, and we will accelerate deployments if we can. We have officers in twelve fusion centers, and we do have an aggressive schedule to deploy up to 35 officers by the end of fiscal year 2008, and that will be a challenge as you pointed out in your comments, and I will be happy to try to respond to questions.

We also realize there is a critical need to provide the physical infrastructure and technology to share that information. At the secret level, my office is deploying a homeland security data network, HSDN, to the fusion centers. The Department is giving direct access, not just to my officers, but to State and local officials, just as if they were working at the Federal level. The establishment of a homeland security information portal and the deployment of HSDN are major steps to increasing connectivity between DHS intelligence and our State and local partners.

We are beginning to realize the benefits of the strengthened relationships that the State and Local Fusion Center Program is creating, especially in creating new information into the centers. We recently assisted a West Coast fusion center in establishing solid information links to extremists operating outside of the United States by connecting informing from local investigators with senior intelligence analysts in my office.

I share many of the concerns expressed by the committee at the last hearing about creating the sustainable fusion center capability at non Federal levels. You are absolutely right. There are going to be challenges, and these centers are in various stages of development. Some are immature, and some are like the JRIC in Norwalk near Los Angeles, which is very mature.

I will defer my comments on radicalization but look forward to any questions. A number of the committee members remarked on the challenges that remain in being able to disseminate intelligence to those who need it, especially State and local partners, including a continuing proclivity toward overclassifying intelligence. I have fought against this tendency throughout my career while trying to ensure we protect sources and methods.

As I noted previously, I look forward to working on this issue with the committee because my primary customers, whether in the State, the private sector or the Department, require intelligence shared with them at unclassified and at secret levels. If there is top secret level, we can sanitize it to secret if there are warning threat assessment necessities.

In conclusion, the United States and its allies are engaged in a continual global struggle against a broad range of transnational threats. While the Department of Homeland Security intelligence is still maturing, we are undertaking vitally important new initiatives such as a State and Local Fusion Center Program to accomplish the Department's mission of preventing and mitigating those threats. While our fusion center initiatives are advancing, invaluable, seamless partnerships are fusing information intelligence. This will be done—I can assure you—while working hard to safeguard privacy and civil liberties. The success of these initiatives is based on DHS intelligence, setting the standards of inclusiveness, access, and collaboration with all of our partners.

I look forward to your questions.

Ms. HARMAN. Thank you, Mr. Allen.

[The statement of Mr. Allen follows:]

#### PREPARED STATEMENT OF CHARLES E. ALLEN

##### *Introduction*

Chairwoman Harman, Ranking Member Reichert, and Members of the Subcommittee: Let me start by saying how pleased I am to be back before your Subcommittee—your continued focus on the critical capabilities that DHS Intelligence provides to the security of our homeland is further evidence of the commitment you have shown to our programs. I thank you greatly for your ongoing support.

I would like to provide an update on our progress in establishing the Interagency Threat Assessment and Coordination Group, which is now called the Federal Coordinating Group. This group will facilitate the production of “federal coordinated information,” ensuring our non-Federal partners have the validated, accurate, timely, and actionable information they need to protect against the threat of terrorism. I am pleased to announce that since I last spoke with you a month ago, we have begun moving staff officers, who form a core advance team, into our location in Liberty Crossing and are working with our Federal and non-Federal partners to fully staff the group. We have a substantial opportunity to construct lasting coordinated solutions by working together. The Federal Coordinating Group's advance team is gathering momentum; each day brings new substantive steps forward. I want to thank both the legislative and executive branches for helping to further the President's vision for information sharing.

Today, I would first like to touch on the highlights of how the Department's State and Local Fusion Center (SLFC) program, and other key initiatives in our proposed FY 2008 budget, promote information sharing both horizontally between fusion centers and vertically to the Intelligence Community, all the while safeguarding civil liberties.

##### *Civil Liberties and Privacy*

Protecting privacy and civil liberties remains one of my top organizational priorities as we work in our homeland security intelligence domain. I hold my Office to the highest standards in these areas and continually reinforce these principles with my senior managers and with all of our employees. I am also mandating that our new programs, such as the State and Local Fusion Center program, incorporate appropriate safeguards and oversight in these areas that intersect with homeland security.

I echo the Secretary's vision that effective tools and measures, such as training, should be developed to safeguard privacy and civil liberties. In terms of incorporating privacy and civil liberties training into our fusion center program, the Department of Justice (DOJ) has made enormous efforts to establish and provide these very important training and outreach programs directed to fusion center personnel. The Global Justice Fusion Center Guidelines published by DHS, DOJ, and participating state and local governments require fusion centers to create policies to protect the civil liberties of our citizens. Fusion centers have to adhere to these guidelines in order to receive Federal grants. Also, all four regional fusion center conferences last year had plenary sessions addressing these issues. The National Fusion Center conference, held last week in Destin, Florida, brought subject matter experts from across the United States, including from the Department's Office for Civil

Rights and Civil Liberties, and one of the issues discussed was privacy and civil liberties. In addition, all Federal intelligence officers assigned to fusion centers must comply with the policy obligations of their agencies concerning annual training requirements on the procedures that must be followed in handling U.S. Person information, as well as abiding by the privacy guidelines of the information sharing environment. To that end, we will continue to work closely, within the Department, with the Office of the General Counsel, the Office for Civil Rights and Civil Liberties, and the DHS Chief Privacy Officer, and, outside the Department, with the President's Privacy and Civil Liberties Oversight Board, the Information Sharing Environment Privacy Guidelines Committee, and other Federal partners to ensure adequate oversight in these areas and to identify where additional training opportunities exist, so that all fusion center personnel understand and abide by the appropriate guidelines.

Madam Chairwoman, the last time I appeared before the Subcommittee, you shared your three priorities with me: information sharing with first preventers; the potential for radicalization within our society; and finding ways to reduce the overclassification of intelligence. As you know, I share your concern in these three areas. I will now describe how the SLFC program and other key initiatives in our proposed FY 2008 budget will emphasize those priorities.

#### *Information Sharing with First Preventers*

New Director of National Intelligence (DNI) Mike McConnell recently set forth his vision to the Intelligence Community for information sharing, stating that we all share a "responsibility to provide." When I last spoke with you, I pledged that DHS Intelligence would set the standard in this area. Our fusion center program and other initiatives in our FY 2008 budget underscore the importance I place on supporting the programs and technology required to increase our contributions to information sharing, especially with first preventers.

The Department created the State and Local Fusion Center program, part of the larger national network of fusion centers, nine months ago, working closely with both the DNI and DOJ. As you know, the program embeds DHS homeland security intelligence professionals into state and local fusion centers to share information, collaborate on analysis, and identify information of intelligence value. My officers continue to work with the intelligence officers of DHS operating components, with our partners at the FBI, and with the national Intelligence Community to move tailored, timely, and actionable intelligence out to the fusion centers. The result is better reporting and validating of actionable information both to our state and local partners and to the Intelligence Community.

We are beginning to realize the benefits of the strengthened relationships the State and Local Fusion Center program is creating with our non-Federal partners. For example, we recently assisted a west coast fusion center in developing what at first appeared to be a tenuous connection with extremist activity. We were, however, able to establish a solid link to extremist activity operating outside of the United States by connecting information from local investigators with our senior DHS intelligence analysts.

The State and Local Fusion Center program to deploy our intelligence analysts to fusion centers around the country is progressing well, although I will look for opportunities to accelerate the deployment of additional officers. So far, we have deployed 12 officers to 12 fusion centers around the country; we are in the process of identifying the next five officers to deploy. We will continue our aggressive schedule to deploy at least 35 officers by the end of FY 2008, and we are continuing to conduct assessments to determine which centers have the greatest need. Madam Chairwoman, I fully expect to meet that goal.

We also realize there is a major need to provide the physical infrastructure and information management technology to share intelligence reporting and analytical products. At the controlled or sensitive but unclassified level, we have established a pilot program capability, under the Homeland Security Information Network (HSIN), that includes an intelligence portal where we comprehensively post both intelligence reporting and analytical products at the controlled unclassified level. We plan to expand this portal to allow for email exchange for states to collaborate while being protected from intrusion. At the SECRET level, my Office, in full coordination with the Department's Chief Information Officer, is deploying the Homeland Secure Data Network (HSDN) to the fusion centers. In an unprecedented move for the Federal government, the Department is giving state and local officials direct access, in their own facilities, to this network so they can receive reporting and email not only from the Department but also from the rest of the Intelligence Community. In other words, state and local officials will have access to and operate on the HSDN net-

work, just like intelligence analysts at the Federal level. The establishment of the HSIN portal (controlled unclassified level) and the deployment of HSDN (SECRET level) are major steps forward in increasing the connectivity between DHS Intelligence and our partners at the state and local level.

Using these mechanisms, we are piping information into the State and Local Fusion Centers at levels that before were not available to non-Federal partners. This information includes international events and incidents that are of concern from the standpoint of lessons learned and situational awareness. For example, we recently provided information and updates to fusion centers on the India train bombing, the Iraq chlorine attacks, and a white powder scare at Rolla, Missouri.

I share many of the concerns expressed by the Subcommittee at my last hearing about creating a sustainable fusion center capability at the non-Federal level. DHS, in partnership with DOJ, is a major supporter of these fusion centers through our grants and accompanying technical assistance and training process, and in providing classified infrastructure, such as secure telephones and fax machines, HSDN terminals, and SECRET clearances to non-Federal homeland security professionals. At the same time, we must look to the future and, with our non-Federal partners, determine how to build both the Federal and non-Federal parts of the President's national integrated network of fusion centers in such a manner that this capability will remain robust, effective, and efficient throughout the protracted campaign against those who seek to harm the United States. In order to support the capability of the fusion centers, I am considering how the Federal government could use retired annuitants—retired intelligence officers who are experienced in intelligence analysis and production. We are reviewing this approach and will assess its feasibility.

#### *Radicalization*

Chairwoman Harman, you recently remarked about the threat that homegrown radicalization poses to our communities. I sincerely share this concern, as does the Department and the broader Intelligence Community, especially the FBI. In fact, my office has followed suit with other Intelligence Community agencies that have realigned their analytical core to focus on radicalization. I am proud to convey that we are beginning to map out the phenomenon in its various domestic forms. This is part of my larger goal of developing indicators for radicalization, which will act as strategic warning when disseminated to state and local partners so they can determine the best ways to alleviate the threat. To assist with their efforts, the Radicalization and Engagement Working Group within DHS is developing a battery of programs and best practices to effectively counter radicalization, which will be available to our non-Federal partners.

My Office's branch that analyzes radicalization has undertaken a study of each region in the United States and the threat radicalization poses. Our assessments of radicalization are being conducted in a phased approach, examining radicalization dynamics in key geographic regions throughout the country. Our first phase assessed radicalization in California and the New York/New Jersey area, and our second phase is assessing the Midwest and the National Capital Region.

Each regional assessment begins by framing the issue particular to that state or region. First, we examine national-level intelligence reporting and open source information. We then take those findings and share them during face-to-face meetings with our Federal partners, including the FBI and the Federal Bureau of Prisons, as well as state and local law enforcement, intelligence, and homeland security professionals to gain their insights. These regional studies will form the basis of a national radicalization study that lays out the first ever baseline of this threat to homeland security.

As you can see through our methodology, our approach to radicalization is indicative of my commitment to engage our intelligence colleagues in the state and local fusion centers as equals, as we address this particularly challenging issue. My radicalization team has been on the road many times in the past year, including attending the national conference in Florida I alluded to earlier, in order to meet with experts in your constituencies and solicit their involvement in our analytic efforts. I previously mentioned the results of the strong partnership with the state of California and similar relationships are supporting our work in all of our regional assessments.

#### *Overclassification*

A number of the Committee's members have remarked on the challenges that remain in being able to disseminate intelligence to those who need it—especially state and local partners. Foremost among those challenges is a continuing proclivity to-

ward overclassifying intelligence. As a long-standing senior officer of the Intelligence Community, I have fought against this tendency throughout my career while consistently ensuring that we protect our intelligence sources and methods to avoid harming our national security. As I noted previously, I look forward to working on this issue with the Committee in no small part because my primary customers, whether in the Department or in the states or private sector, require intelligence shared with them at the UNCLASSIFIED or at most SECRET levels. I will always ensure we share threat information with those consumers that require it—and my staff and I are working hard to institutionalize the DNI's principle of “responsibility to provide” in our own efforts to support this approach throughout the community. I believe the Information Sharing Environment Program Manager, in implementing the President's guidelines, is taking numerous steps forward in this area, and I will continue to support him.

Within the Department, I have a strong production management team working to disseminate our finished intelligence at the lowest level possible to ensure wide accessibility by those who need it to secure our homeland. As I noted before, we made investments and will continue to invest in laying the connectivity at both the Controlled UNCLASSIFIED level through HSIN (and especially our HSIN-Intelligence portal, which has proven to be a success) and at the SECRET level through HSDN. Equally as important, I have instructed my analysts to “write for release” at the lowest possible level and to work with our partners in the Intelligence Community to release information they are providing to levels accessible for our customers.

Much work remains to be done—the President's guidelines lay out the roadmap for much of our efforts in this area. Within the Intelligence Community, DNI McConnell's principle of “responsibility to provide” further directs our approach. I will work closely with Mike McConnell and with you to ensure we are providing the right information to our customers on a timely basis to secure our homeland.

While today I am focusing on the State and Local Fusion Center program and other key activities that intersect with the priorities you laid out for the Subcommittee, I want to emphasize that our FY 2008 program provides capabilities in all of our mission areas. The program includes new initiatives such as our Domestic Open Source Intelligence Enterprise, our partnership with U.S. Citizenship and Immigration Services via the new National Immigration Information Sharing Office, and our work to support border security through the Integrated Border Intelligence Program. I ask for your continued support for the full range of capabilities and initiatives included in the FY 2008 budget—I will need this program fully funded in order to deliver on the pledges I made to you, the Secretary, the DNI, and to the country. Before I conclude, I would like to touch on a few final areas that are imperative to our success.

### *Risks*

In my February 14 testimony, I shared with you three risks that are having deleterious effects on our ability to provide results: recruiting and retention; integration; and facilities. While I remain concerned about all three, today I want to focus on a key aspect of integration: the challenge of providing sound management of the Department's intelligence investments, including the SLFC program.

As you know, we have seven components in the Department with intelligence programs, collectively called “the DHS Intelligence Enterprise.” We also have a host of places in the Department undertaking intelligence-related activities, some of which are programmatically positioned outside the intelligence components. The Secretary has charged me, as Chief Intelligence Officer, to advise him on the intelligence investments in the Department to ensure we are making effective and efficient investments in our intelligence capability.

To this end, I am working aggressively to gauge accurately the cross-departmental component expenditures on intelligence. The first ever DHS Intelligence program reviews conducted last year were an important step toward gaining a baseline understanding of the intelligence component investments across the Department. These program reviews, as well as information gathered in partnership with the Chief Financial Officer during the Resource Allocation Plan process last year, provided a fair amount of visibility into the total departmental planned expenditures in the intelligence components. This year, I will again conduct intelligence program reviews and will again, in partnership with the Chief Financial Officer during the Resource Allocation Plan (RAP) process, gather information on planned investments in the intelligence components. The outcome of this year's activities will enable my staff to validate the results of the previous year's analysis. After this second set of program reviews and the FY 2009 RAP process, I will be able to provide a more accurate

estimate of the current and planned expenditures of the DHS Intelligence Enterprise.

One of the challenges I am facing is that because the intelligence expenditures across the Department are not necessarily tracked at the program level—some operating agencies, for example, do not line item their intelligence component budgets—the final analysis will still only produce an estimate of investments. Similarly, because some agencies have intelligence resources that are organizationally distinct from their component intelligence program, these intelligence investments are difficult to estimate at the current time. As a result, I am still not able to provide the level of accuracy I prefer in my recommendations to the Secretary on current and proposed intelligence investments across the Department. I am working with the Secretary to improve our methodology toward this challenging and important issue, and I will continue to update the Subcommittee on my success in instilling an integrated approach to managing the Department's intelligence investments.

#### Conclusion

The United States and its allies are engaged in a continuing, global struggle against a broad range of transnational threats. Our nation's communities face the threat of terrorism, of cross-border violence fomented by illicit narcotics trafficking and alien smuggling, and other threats apart from terrorism. While DHS Intelligence is a modestly-sized program, we are undertaking vitally important initiatives, such as the State and Local Fusion Center Program, to accomplish the Department's mission of preventing and mitigating these threats. The success of these initiatives is based on the degree to which DHS Intelligence sets the standard for inclusiveness, access, and collaboration with all of our partners.

I can assure you that DHS Intelligence will be relentless in its pursuit of excellence in supporting the homeland security mission. With this budget, we will exceed past accomplishments and levels of customer service and collaboration—our “responsibility to provide.” At the same time, we will ensure that our intelligence programs protect the civil rights and civil liberties of all Americans. Our nation—our communities, our families, our way of life—deserves nothing less.

Ms. HARMAN. I yield myself 5 minutes for questions.

You just mentioned that there will be growth in State and local representation at the ITAG, which is now renamed or will be renamed the Federal Coordination Group.

Did you say that? Am I correct?

Mr. ALLEN. That is correct, the Federal Coordinating Group. The Information Sharing Environment Program Manager has decreed that is the name. At least, when I saw him on Monday, I think that is what we called it.

Ms. HARMAN. Okay. Well, the name is less important than the function. We can agree on that.

My question is what you mean by growth in State and local representation. Why can't the entity start with more than one law enforcement officer, which I think all of us here would believe is important.

Mr. ALLEN. As we finish our concept of operations and as we work out the roles and responsibilities in that concept of operations, I think you will find that there will be more representatives than, say, one, and I do not know where the issue of “one” came from, but we are going to work with the chiefs of major cities' police. We are going to work with the global justice—I cannot remember the name—the Global Justice Committee, in order to ensure that we get the fullest input because we want the State and local representatives to represent all of the State and local fusion centers and local police departments at large, that we do not look each of the cities and other fusion centers and send in officers at the local level. We want people there who can help our Federal intelligence analysts understand what is important. Can it advise Fed-



eral analysts? You know, this foundation document on terrorism techniques, tactics and procedures, that is going to be very helpful at the local level, and so these people are going to be very crucial to our performance.

Ms. HARMAN. Well, you are talking the talk, but I urge you to walk the walk. I would strongly recommend that more than one law enforcement officer be part of the initial group of people. Surely, there is more than one qualified law enforcement officer you could include, and I would hope they would be recommended by the State and local groups, themselves, not by you. I mean, that does compromise the idea, but also, if you call this the Federal Coordinating Group, I think that may send the wrong message, too. I think the point is to improve information sharing and to help get the perspective from State and locals on what products would be useful and what insights they have.

So I do not want to name the thing, and I am not sure I recall what "ITACG" stood for, but the point is to take advantage of the talent pool out there, and I think you will agree with me, so I urge you to take advantage of more of the talent pool out there.

Let me turn to a couple of other subjects that you raised. You were talking about these guidelines for civil liberties that the Justice Department has.

My question is: Are these guidelines mandatory or voluntary?

Mr. ALLEN. These guidelines are recommended by Justice, by our own department, working those guidelines out with State and local. We believe that State and local fusion centers will follow these guidelines because they understand it is very important that they meet high standards for the protection of civil liberties, and I think, you know, that would affect our opinion and our assessment because, before we put officers into any fusion center, I send at least three or four officers out, and they spend several days evaluating how that center is forming, and that is one of the places where they put a lot of emphasis.

Ms. HARMAN. Right.

Mr. ALLEN. They have to meet those standards.

Ms. HARMAN. Well, I will just point out that H.R. 1, which has passed the House and has passed the Senate just this week in a different form—H.R. 1 does include a provision that would make those mandatory. Obviously, we share the goal of making sure that they are the right standards and that they are followed.

Finally, let me ask you about budget. I understand that the budget is classified. I am not asking you to reveal any details of it, nor will we, but you said it would be a challenge to meet your goal of getting personnel into 40 fusion centers.

Could an increase in budget be helpful in that regard?

Mr. ALLEN. My view is, when we formed our program for fiscal year 2008 through 2012, I had just arrived. We had begun a number of new initiatives. We had not embedded anybody. We did not have a State and local program office. We now have that. As you know, we have started a number of other new initiatives within DHS intelligence. I think we are going to be very challenged. It may require me to reallocate dollars within my overall budget in order to meet some of these demands such as the State and Local

Government Office. There are other initiatives of which your staff has been briefed that will require additional resources.

Ms. HARMAN. Right. So I am not sure whether you said "yes" or "no," but let me just—my time has expired.

Would additional resources be helpful?

Mr. ALLEN. We always welcome additional resources.

Ms. HARMAN. Thank you. Thank you. I appreciate that.

I now yield 5 minutes for questions to the Ranking Member.

Mr. REICHERT. Thank you, Madam Chair. That is the same answer the sheriff would have given to the county council. You always can use more resources.

As we look at the ITACG, and you look at bringing local law enforcement in, are you experiencing any resistance to volunteers or people who might be interested in that position?

Mr. ALLEN. I do not think there is going to be any shortage of people wanting to come to Washington to work at Liberty Crossing to help in sanitizing, taking away sources and methods if need be and pushing the information out hopefully at official use or sensitive but unclassified or law enforcement sensitive levels down to there or, if need be, at secret levels. I think we are going to have a surfeit of people wanting to do this. I know that a number of cities have volunteered to send officers. Dave Cohen in New York has done so.

Mr. REICHERT. Good. I do agree that the opportunity would be one that a local law enforcement officer would love to participate in, but more toward the budget side in consideration for those other cities that might have a little bit smaller police force, these are positions that are volunteered to the Federal Government to serve in this capacity on a temporary basis; is that correct?

Mr. ALLEN. That is correct.

Mr. REICHERT. Is there any Federal reimbursement at all to the local agency providing the body?

Mr. ALLEN. We have not worked that out, but I certainly would think that that would be appropriate to reimburse, to pay for their moving expenditures and what have you, because it seems to me, if we are going to have a "Federal Coordinating Group," we ought to reach out and give a helping hand to those coming from State and local governments.

Mr. REICHERT. Would the wages be a cost that might be a burden that the Federal Government carry or would that still apply to the local agency?

Mr. ALLEN. We have to work that out. That is a policy decision yet to be reached, and we have to do that in cooperation with the DNI—with the Director of National Intelligence—as well as with the FBI.

Mr. REICHERT. I do know there has been some resistance to fund positions at fusion centers and joint analytical centers and JTTFs. Do you know if there has been any further discussion on whether or not monies could be found maybe within the grants and training?

Mr. ALLEN. I think we can look at our grants and trainings because we know that grants and training funds can be used, for example, by the fusion centers to hire analysts. They can hire contractors to come in as analysts, and they actually can use some of

the grant monies to actually train those analysts in analytic trade craft, so I will have to look into it, but there is flexibility there.

Mr. REICHERT. It has been one of the big issues that local law enforcement agencies in cities and counties across the country have expressed over and over again, you know, removing, as I said in my opening statement, resources from a gang unit, for example, to participate in a fusion center experience, where I think that their input and participation is absolutely vital for the success of that fusion center or analytical center.

Just to touch on the privacy issue very quickly, to your knowledge, have there been any demonstrated privacy or civil liberties issues with any of the fusion centers?

Mr. ALLEN. I cannot speak for all of the fusion centers, because there are areas where we really have not visited some of the fusion centers. We certainly have visited the State of Washington, as you know.

Mr. REICHERT. Yes.

Mr. ALLEN. But where we have officers embedded, we have asked them to report any concerns they may have, and in the twelve fusion centers, we have received no reports of any concerns. That is certainly going to be part and parcel of sending officers to the fusion centers, all of the civil liberties and privacy rules and guidelines we expect those centers to follow.

Mr. REICHERT. One last question in my minute, remaining.

Are you aware of the policy or the request that the Federal Government has made for phone records of American citizens? Are you familiar with that? It was an issue about 5 or 6 months ago or so.

Mr. ALLEN. I am not familiar with any requests.

The Department of Homeland Security, our Customs and Border Patrol and Transportation Security Administration and Immigration and Customs enforcement can collect information. In my own office, we do not collect information. We get the information that they provide, but all of the information is collected lawfully at ports of entry.

Mr. REICHERT. Okay. I yield.

Ms. HARMAN. Thank you, Mr. Reichert.

I would just note that there are programs. There is a program that involves the collection of some phone records, but it is not administered by the Department of Homeland Security; it is administered in other ways, and much about that program is classified, and certainly, I would hope that all of it complies fully with our law. Let me just leave it there.

The Chair now recognizes for 5 minutes the gentleman from Washington State, Mr. Dicks.

I would just note for the record that we do plan to come to Washington State for a field hearing. Both the ranking member and Mr. Dicks will be part of that hearing if we can find a mutually convenient date. We are also going to Los Angeles on April 4th and 5th to revisit the JRIC, the Joint Regional Intelligence Center, and hold a field hearing on radicalization and information sharing, and we will be meeting, Charlie, with your detailee out in Los Angeles at that time.

Mr. ALLEN. Yes. The Secretary has asked me to try to attend that if I could.

Ms. HARMAN. Wonderful. We will welcome you. We had thought you were unavailable, but that would be great.

Mr. ALLEN. I will look at my schedule. I would like to make that.

Ms. HARMAN. Terrific.

Now, Mr. Dicks, you are recognized for 5 minutes.

Mr. DICKS. I think this fusion center idea is a good idea. I mean I am very supportive of this, and I am glad that we have gotten started with twelve, and we are going to build this national network.

Could you provide some specific examples of how fusion centers have improved homeland security and how your staffs present at fusion centers has made things better?

Mr. ALLEN. Yes, sir.

For example, when the President talked about some of the disrupted terrorist plots, the library tower in Los Angeles was mentioned as one plot where Khalid Sheik Mohammed had planned that. That was not pre cleared, necessarily, directly with the Mayor of Los Angeles. It was cleared at many levels below that, but our having an officer embedded there to talk quickly to all of the officials at the senior levels I think helped ease some of those pains.

The point is we get every day, as you know, Congressman Dicks, threats. I got one last night which I called home on, and we are able then to—most of them are rumors or non credible. There are some that are credible. We are able to separate the wheat from the chaff, and having that officer there with a secure phone or a secure data network makes all of the difference in the world, and we have been able to do it with UNIRIC up in New York and other places.

Mr. DICKS. And the way the thing is structured, you have these fusion centers out there in the local communities, and then you have your—what do you call it?

Mr. ALLEN. We have the homeland security data network, which is a secret level that has all of the robustness of a Department of Defense supernet capability.

Mr. DICKS. And then you have an office here in Washington, D.C.; is that correct?

Mr. ALLEN. We are forming—yes, we have a State and local government program office that is now being properly classified and so forth at the various levels, and we are selecting a senior officer to head it.

Mr. DICKS. And so the idea is for information to move both directions—out to the states and locals from here and then information from there coming back here?

Mr. ALLEN. Absolutely. My Deputy Assistant Secretary for Intelligence this morning told me that her senior intelligence officers—and we have quite a number of them—are receiving every day calls from State fusion centers, not just where we have embedded officers but around the country. They have our number, and they are calling us if they have concerns.

Mr. DICKS. And you said you have a data transmission system linked up, too, right?

Mr. ALLEN. Absolutely, at all of the places except the upper New York regional intelligence center, and that will be in within a month. I discussed that yesterday to get that up to Colonel Bart Johnson.

Mr. DICKS. And you have a plan to go to how many, 36?

Mr. ALLEN. We want to put people out in 35 plus, and as the chairwoman said, we are going to be challenged to get that all out there by the end of fiscal year 2008.

Mr. DICKS. That is your goal is to try to do it by 2008?

Mr. ALLEN. Yes, sir.

Mr. DICKS. And that is where the possibility of additional funding would maybe help to do that?

Mr. ALLEN. We have undertaken a number of new initiatives that your staff has been briefed on, and we probably are going to have another new initiative coming on, perhaps on counterintelligence, that will require some money, which I am doing in conjunction with the Director of Security. So, yes, we are taking on some real initiatives, sir, that I think are needed.

Mr. DICKS. Give me an example of where you would be concerned about civil liberties and, you know, how you would want to safeguard them.

Mr. ALLEN. Hypothetically, I could say, having lived through a bit of Vietnam and knowing some of the abuses that occurred then where people went out and not only videotaped or filmed any war demonstrations but tried to get additional data on those people—if it is a peaceful protest where there is no reasonable belief under Executive Order 12333 that any of these people are planning any interference activity against the United States at any level, I always think that that would be an abuse. You do not do that. People have the right to protest.

Mr. DICKS. We had some protest out in the State of Washington just last weekend at the Port of Tacoma regarding, you know, Stryker vehicles being sent to the war in Iraq. I mean, these are all going to be judgment calls that people are going to have to make, and that is why you are emphasizing the training aspect of this.

Mr. ALLEN. If we do not have training, there will be abuses. If we do not have training at the local and State levels and they do not meet Federal standards and guidelines, I think there will be abuses, so I think we have to work rigorously at the training part.

Mr. DICKS. Is there a set of required people in a fusion center or do we kind of make it up as we go in each area? I heard the idea of one law enforcement person, but I mean, who is supposed to be in the fusion center, and I know you are going to have your representative there, but who else would be in one of these existing centers?

Mr. ALLEN. Some of these are collocated with the Joint Terrorism Task Force of the FBI. Some are located at Emergency Operations Centers. Some are located with State police. So we have a variety of people. They bring people—

Mr. DICKS. So there is no set—

Mr. ALLEN. No, because there is no one cookie cutter approach to State and local fusion centers. These have grown up as a result of 9/11, and the people at the local level are feeling that they had to have a more coordinated way to look at problems within their own communities.

Mr. DICKS. Thank you.

Thank you.

Ms. HARMAN. Thank you, Mr. Dicks.

The Chair now recognizes for 5 minutes the gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thanks, Madam Chairman.

Nice to see you again, Mr. Allen. The question I have is the House Appropriations Committee is proposing an additional \$35 million in the fiscal year 2007 supplemental for the expansion of the fusion center initiative.

How is this funding level going to help you expand and strengthen the program, including privacy and civil liberties programs?

Mr. ALLEN. Well, Congressman, as you know, that would be an action taken by House Appropriations.

Mr. DENT. Correct.

Mr. ALLEN. It is not part of the President's budget or the Secretary's budget that we submitted.

As I said, we will be very challenged to meet some of our goals. We actually will be able to meet our goals, but we may not be able to fulfill all of our other initiatives. So, you know, it is your wisdom as to how to allocate any additional funds. We certainly are not going—I certainly cannot say truthfully to you that I am going to be very much squeezed, and I believe the State and local fusion center initiative is so important that I am willing to sacrifice other initiatives, if necessary, to meet the goal of embedding officers at 35 major fusion centers by the end of fiscal year 2008.

Mr. DENT. Well, thank you for that answer.

How would you work to increase public awareness through outreach between fusion center personnel and key community leaders to help create that trust between law enforcement and communities on this whole fusion center issue?

Mr. ALLEN. Well, certainly at State and local fusion centers and with the major police departments where we also do a close liaison both in New York and out in Los Angeles, for example. Those centers and those police departments do have outreach programs to the local community. Part of our problem—part of our challenge, of course, is to get our officers out and serving and explaining the kind of information we can provide to help keep the community safe. We have officers who are very active in some of the centers and who know all of the key players within the community, and the information we provide is threat warning, threat assessment and these more foundational documents, so I think we are building a center of trust down there. The State and local fusion centers have a prime responsibility for outreach to their local communities.

Mr. DENT. Thank you, and thank you again for your extraordinary service.

I yield back.

Ms. HARMAN. Thank you, Mr. Dent.

I am not sure whether members are interested in a second round of questions or not. Is anyone interested in asking some more questions?

All right. Well then, we will need a few minutes to move to our second panel, but I just would like to say to you, Mr. Allen, that your careful answers to our budget questions are noted, but we believe that it would be helpful to give you some resources to make this fusion center concept a more effective one. Fusion centers are

the way not only to share information vertically, which has been drawn out in this conversation, but also to share information horizontally at the local level, and that was something that the members who went to the MCAC in Baltimore learned on Monday, and I actually saw one of the products that is used, which was fascinating because it had information in this Baltimore document about some activity that could be happening in Los Angeles early next week, and that information was being shared with the Joint Regional Intelligence Center—the JRIC—of the fusion center in Los Angeles, and so, if we do this right, information will flow seamlessly, as we say, on a horizontal basis at the Federal level, but also seamlessly vertically and seamlessly among the State and local fusion centers, and that will maximize the chance, I hope, that we will connect the dots the next time before any attack on U.S. interests or U.S. persons. So this is very promising. We know that you are our partner in this, and all of us here are dedicated to making this succeed.

Thank you for your testimony.

Mr. ALLEN. Thank you, Madam Chairman.

Ms. HARMAN. Mr. Reichert, do you have anything to add?

Mr. REICHERT. What the Chairwoman said. Thanks.

Ms. HARMAN. This is a lovely exercise in bipartisanship. Thank you, Mr. Allen.

Mr. ALLEN. I am very grateful.

Ms. HARMAN. Are we ready? Okay. The subcommittee welcomes the second panel of witnesses.

Our first witness, Daniel Sutherland, is the Department's Officer for Civil Rights and Civil Liberties. Mr. Sutherland provides advice to Secretary Chertoff and to the senior officers of the Department on a full range of civil rights and civil liberties issues. He has been a civil rights attorney throughout his legal career, serving 14 years with the Civil Rights Division of the Justice Department and nearly 2 years with the Office For Civil Rights at the U.S. Department of Education.

Our second witness, Hugo Teufel is the Department's Privacy Officer. Mr. Teufel has primary responsibility for privacy policy at the Department that includes ensuring that the technologies used by the Department are privacy-compliant, conducting privacy impact assessments of proposed rules at the Department, assuring that the Department, itself, complies with the Privacy Act, and reporting to Congress on the activities of the Department that affect privacy.

Before joining the Privacy Office, Mr. Teufel served as the first Associate General Counsel for General Law at the Department. He also previously served as the Associate Solicitor for General Law at the Department of the Interior.

Ms. HARMAN. Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his statement for 5 minutes beginning with Mr. Sutherland.

Welcome.

**STATEMENT OF DANIEL W. SUTHERLAND, OFFICER FOR CIVIL RIGHTS AND CIVIL LIBERTIES, DEPARTMENT OF HOMELAND SECURITY**

Mr. SUTHERLAND. Thank you, Chairwoman Harman and Ranking Member Reichert. It is a pleasure to testify alongside Hugo Teufel, who has been a good colleague and friend for a number of years at the Department, and our offices work closely together, and we hope that that comes across today as we talk.

I just wanted to describe at the beginning the purpose or mission of our particular office in accordance with 6 USC 345, the statute that creates our office. Our mission is to assist our colleagues in the Department of Homeland Security to secure our country while also preserving our freedoms and our way of life. In essence, we are providing guidance to our colleagues at the intersection of homeland security and civil rights and civil liberties. We, therefore, have the opportunity to work closely with every DHS component. I recently looked at the organization chart for the Department and noted that we have a project with essentially every box on the organization chart, and I am sure that that is the same with the Privacy Office.

We also work with field offices around the country. We worked on nearly all aspects of the issues and the homeland security effort from the Hurricane Katrina recovery to the operation of Watch List to the immigration policy to the training of our workforce.

We believe that our work is supported by our other colleagues in the Department because we try to provide constructive and proactive advice that allows them, our colleagues, to do their work in the most effective way possible. Our work has also been welcomed by our colleagues outside of government as demonstrated by our frequent collaborations with civil rights and civil liberties organizations. We play a unique role within the Department and, we hope, a valuable one, and we are going to continue to try to assist our colleagues as we sort through the issues again that are at the intersection of homeland security and civil rights and civil liberties.

Because our office is relatively small, we realize that, to use a sports analogy, we have to "punch above our weight," and one of the ways that we have decided to expand our influence is to work on training issues, and we have created a program we call Civil Liberties University, which is basically a program to provide high-quality training on a wide range of topics. Through Civil Liberties University, we have developed a video that emphasizes the elements of the National Detention Standards for protecting immigrant detainees. We have a multi-hour instructional video on how to screen people with disabilities at airports.

We have done training on Constitution Day to try and emphasize the value of the Constitution. We have also developed written materials on how to screen people who wear religious head coverings, for example, people who are Sikh or people who are Muslim. We have also developed materials on people who are Sikh who carry the kirpan—a ceremonial, religious dagger—and a number of other issues like that.

We have just released an intensive training DVD on the issue of how to relate to Arab and Muslim travelers, travelers from the Arab and Muslim world or Arab Americans and Muslim Americans.



It is a training that involves insights from four experts—one a Muslim woman who is on the National Security Council, one a Muslim Federal prosecutor, one a member of a civil rights organization that represents Arab and Muslim community interests, and one a prominent Islamic scholar. We have also developed training on the issue of racial profiling, racial or ethnic profiling. When can you use race or ethnicity in the course of law enforcement activities? It is a tutorial that our people take, and they have to pass certain tests as they go through the training.

So the bottom line, I think, is that we have decided that training is a way that we can help make an impact on something that is really being welcomed by our colleagues across the Department. So, just for the better understanding of the role of the office and our training program, I just want to make a couple of comments about fusion centers.

Just one week ago today, as you mentioned, we had the National Fusion Center Conference, and Secretary Chertoff at that conference said that the protection of civil liberties must be a priority, and he outlined the Department's vision in fusion centers, including the need to develop thoughtful tools and measures to safeguard privacy and civil liberties. So, again, I think we are all on the same page in terms of the priorities of these issues. Our office has worked on a number of issues regarding fusion centers. For example, just last week at the conference, we delivered or made available over 600 copies of that Arab and Muslim culture video training to members of the fusion—to people involved in fusion centers around the country. We have also worked on different policy documents that have been developed over the past years.

We know that fusion centers will face a number of issues with regard to civil rights and civil liberties. I have outlined a few of those concerns in my written statement, and I can certainly go over them during the question and answer session, but we just want to make clear that the Office of Civil Rights and Civil Liberties stands ready to assist our colleagues in fusion centers around the country as we have worked with our colleagues within our own department to try to help meet the challenges that they face at the intersection of civil rights and civil liberties in homeland security. I thank you for the opportunity to testify.

Ms. HARMAN. Thank you very much.

[The statement of Mr. Sutherland follows:]

#### PREPARED STATEMENT OF DANIEL W. SUTHERLAND

##### *Introduction*

Chairwoman Harman, Ranking Member Reichert, and distinguished Members of the Subcommittee: Thank you for providing me the opportunity to testify today. The work undertaken in fusion centers across the country will be most successful when it is done in a way that respects America's rich Constitutional history. My colleagues in the Office for Civil Rights and Civil Liberties and I look forward to working with this Subcommittee to ensure that fusion centers reach that highest level of effectiveness.

##### *Mission of the Office for Civil Rights and Civil Liberties*

In accordance with 6 U.S.C. § 345, the mission of the Office for Civil Rights and Civil Liberties is to assist the dedicated men and women of the Department of Homeland Security to secure our country while preserving our freedoms and our way of life. We assist our colleagues in four ways:

- We provide proactive advice on a wide range of issues, helping the Department to shape policy in ways that are mindful of civil rights and civil liberties;

- We investigate and facilitate the resolution of complaints filed by the public regarding Departmental policies or actions taken by Departmental personnel;
- We provide leadership to the Department's equal employment opportunity programs, seeking to make this Department the model Federal agency; and,
- We serve as an information and communications channel with the public regarding these issues.

In essence, we provide advice to our colleagues on issues at the intersection of homeland security and civil rights and civil liberties. We therefore have the opportunity to work closely with every DHS component, both in Washington, D.C., and in many field offices across the country. Our Office has been involved in nearly all aspects of the critical issues facing the homeland security effort—from the Hurricane Katrina recovery, to the operation of watch lists, to immigration policy, to the training of our workforce. The Office's work has been supported by other DHS elements because we provide constructive advice that allows the men and women of the Department to fulfill their mission at the highest level of effectiveness. Our work has also been welcomed by our colleagues outside of government, as demonstrated by our frequent collaborations with leading civil rights, immigration, and community organizations. Our Office plays a unique role within DHS, and, we hope, a valuable one, and we will continue to assist our colleagues to tackle complex issues in innovative and constructive ways.

#### *The Office for Civil Rights and Civil Liberties' Role in Training*

Because our Office is relatively small (approximately one-twentieth the size of the Department of Justice's Civil Rights Division, for sake of comparison), we realize that we must, to use a sports analogy, "punch above our weight." One of the ways we have expanded our influence is by creating "Civil Liberties University," a program to provide high-quality training on a wide range of topics. Through Civil Liberties University, we have developed: a training video that emphasizes elements of the National Detention Standards, a multi-hour instructional video on how to screen people with disabilities at airports; and, training to commemorate Constitution Day in 2005 and 2006. We have also developed educational materials on how to screen those who wear religious head coverings, and how to screen those of the Sikh faith who carry a *kirpan*, or ceremonial religious dagger. We have just released an intensive training DVD for DHS personnel who interact with Arab Americans, Muslim Americans, and people from the broader Arab and Muslim world. The training includes insights from four experts—an Assistant United States Attorney who is Muslim, a member of the National Security Council who is Muslim, a scholar of Islamic studies, and a civil rights attorney who advocates on issues of concern to Arab American and Muslim American communities. This training program has been applauded by communities who believe that they will be treated with more dignity and professionalism if front-line officers understand their cultures, traditions and values; and, by our colleagues in the Department who have expressed a desire for such training.

Another training product we have developed deals with the issue of racial or ethnic profiling. To achieve President Bush's goal to eliminate racial profiling, the Department of Justice issued "Guidance Regarding the Use of Race By Law Enforcement Agencies" in 2003. Subsequently, then-DHS Secretary Ridge issued a memorandum underscoring DHS's commitment to race neutrality in all law enforcement activities. In the wake of the London bombings in July 2005, and the arrests in London this past August, Secretary Chertoff reiterated DHS's commitment to ensuring full implementation of the DOJ Guidance. To implement these commitments by the President and the Secretary, our Office has worked with the Federal Law Enforcement Training Center (FLETC) to restructure and strengthen the curriculum taught to law enforcement officers on this topic. Moreover, Civil Liberties University also has training on this topic: "Guidance Regarding the Use of Race for Law Enforcement Officers," a tutorial on the DOJ Guidance and the DHS policy. These materials are now available to DHS law enforcement employees in CD-ROM or via on-line web-based training formats.

#### *Civil Liberties and Fusion Center Information Sharing*

With a better understanding of the role of our Office and our training program, let me address the topic of fusion centers and information sharing. Just one week ago today, Secretary Chertoff told the National Fusion Center Conference that the protection of civil liberties must be a priority. He further outlined his vision for the Department's involvement in fusion centers including the need to develop thoughtful tools and measures to safeguard privacy and civil liberties.

The Office for Civil Rights and Civil Liberties has been involved in shaping the work of the fusion centers already in existence. Just last week, our Office made available its training module on Arab and Muslim cultures to nearly 600 fusion cen-

ter directors and local, state, tribal, and federal law enforcement officers within intelligence units attending the National Fusion Center Conference in Florida. Last year, our Office reviewed and concurred with the DHS Support Implementation Plan for State and Local Fusion Centers, which included an acknowledgement of DHS's express role in providing training and exercises for fusion centers through its Office of Intelligence and Analysis.

Our office also plays a role in monitoring information management processes within DHS. In a recent memo to all DHS components, Secretary Chertoff assigned the Office for Civil Rights and Civil Liberties, the Office of General Counsel and the Privacy Office to work with DHS's new Information Sharing Governance Board to ensure that privacy, civil rights and civil liberties are fully protected in the Department's information-management processes.

Fusion centers have been provided with some guidance on the protection of civil rights, civil liberties and, specifically, privacy rights. These guidelines have included policy templates for justice information systems, with important references to the Privacy Act, the Federal Retention Act, Executive Order 12333, and 28 CFR 23, that States can supplement with their own statutes. Going forward, DHS is working with other Federal agencies, on the Privacy Guidelines Committee, to establish a process for ensuring that the policies developed by fusion centers provide protections that are at least as comprehensive as those provided by the recently-issued and Presidentially approved Privacy Guidelines for the Information Sharing Environment.

Nevertheless, fusion centers will continue to face a number of issues with regard to protection of civil rights and civil liberties. These issues include:

- Many fusion centers support all-crimes missions and share information related to concerns such as fraud, racketeering, computer hacking, all hazards, disaster recovery and other issues, not just terrorism information. The more types of information shared, the greater the task for fusion centers to ensure civil liberties and privacy rights are upheld.
- Likewise, the increasing demand for more actionable information to be delivered to non-federal partners has the potential to compound civil liberties concerns. Increased discretionary authority may follow on the heels of demands for such increased actionable information, thereby confusing all parties as to who is responsible to preserve civil liberties and what statutes—Federal, State and local—apply to the information and actions taken.

If sunset provisions for retention of information by a fusion center are absent, this can, depending upon what the information is used for and what security or updating procedures apply to it, become a privacy and civil liberties concern as ever more information is captured, shared and stored. Where provisions and rules for retention are in place, there is still risk that these provisions will not travel with the systems and people who use the data.

As partnership with Federal authorities and non-federal fusion center participants increases, there is increasing risk that the balance between Federal and state governments is disturbed. The Constitution creates a delicate balance between Federal and state governments, which helps to prevent the accumulation of excessive power in either the States or our central government. As the Supreme Court has explained, "The Constitutionally mandated balance of power between the States and the Federal Government was adopted by the Framers to ensure the protection of our fundamental liberties." *Atascadero State Hospital v. Scanlon*, 473 U.S. 234, 242 (1985).

Finally, the accumulation of data leads to a substantial problem of misidentifications. We have observed this problem clearly in the context of travel screening, as many Americans have faced obstacles to flying as a result of misidentifications with names on watch lists. The Department of Homeland Security has acknowledged the issue from the beginning, and worked aggressively to solve it. Most recently, the Department has established an entirely new system to bring redress to travelers, known as DHS TRIP. Without such redress mechanisms, there are serious and unintended consequences to the collection of data.

#### *Fusion Center Training and Monitoring*

The Office for Civil Rights and Civil Liberties, within available resources, stands poised to work with fusion centers to address these and other challenges. While considering our success in training and our track record of close cooperation with every DHS component, we will build upon the framework established by the ISE Privacy Guidelines, and work with DHS's Privacy Office and I&A to protect and preserve privacy and civil liberties in the information sharing environment. Besides assisting these offices and the Department of Justice in monitoring fusion center utilization of Fair Information Practices, we plan to supplement I&A orientation training for DHS participants with civil rights and civil liberties instruction. Conclusion

I thank you for inviting me to share our thoughts on fusion centers today and I look forward to working with this Subcommittee to address these issues.

Ms. HARMAN. Now Mister—is it “Too-fel” or “Toy-fel.”

Mr. TEUFEL. It is “Toy-fel,” ma’am.

Ms. HARMAN. “Toy-fel.”

Would you please summarize your statement in 5 minutes.

**STATEMENT OF HUGO TEUFEL, PRIVACY OFFICER,  
DEPARTMENT OF HOMELAND SECURITY**

Mr. TEUFEL. Absolutely. Madam Chair, Ranking Member Reichert and members of the subcommittee, it is an honor to testify before you here today. I am particularly pleased to be appearing with my good colleague, Dan Sutherland. As the subcommittee knows, our offices have a statutory responsibility to work together to address privacy and civil liberties issues in an integrated and comprehensive manner, and I want to assure you that we do.

Because this is my first time appearing before the subcommittee—in fact, the first time that I have ever testified before any committee at either House—I wanted to mention a couple—

Ms. HARMAN. It is a great honor, I should point out.

Mr. TEUFEL. Yes, ma’am, indeed.

I wanted to mention a couple more things.

When I was Associate General Counsel for General Law, I was very lucky to have as two of my clients, my predecessor, Nuala O’Connor Kelly, and Dan Sutherland. So, in that role, I had the opportunity to have a very good understanding of what both offices do.

Also, I would like to mention to you—I think it is particularly relevant given the Chair’s earlier statements—that previously, I served as Deputy Solicitor General for the State of Colorado, and unfortunately, I see that Representative Perlmutter is not here. My fellow Coloradoan, sadly, is not with us right now, but I did want to mention Colorado since I am here before you all.

The subcommittee has just heard from Assistant Secretary Allen who expressed how important fusion centers are to critical Department missions. He also pointed to the Department’s aggressive plan to increase the number of fusion centers across the Nation. As Chief Privacy Officer, I was gratified to hear the Assistant Secretary’s commitment to establishing sound and effective privacy practices and policies from the very beginning.

In the Privacy Office, we understand that this is more than a compliance issue. Sound and effective privacy policies enhance program performance while minimizing the cost to agencies and to the public. Like the Assistant Secretary, I believe the fusion center guidelines issued by the Global Information Sharing Initiative and published in cooperation between the Department of Justice and the Department of Homeland Security provide an invaluable resource for the principals to utilize when founding and operating a fusion center and will also be helpful to me, as a member of the Information Sharing Environment Privacy Guidelines Committee, in monitoring how privacy is safeguarded in this crucial aspect of the information sharing environment.

The fusion center guidelines encourage consideration of privacy interests from the very moment of formation, a critical step. These

guidelines recommend creating a privacy committee within the governing structure of the fusion center. The participants are encouraged to enter MOUs where privacy and related security protections and responsibilities are specifically called out. The guidelines promote meaningful and lawful privacy policies at the fusion centers and provide mechanisms ensuring that the centers adhere to these policies. Security is also addressed because it is well-understood in the privacy community that security concerns become privacy problems. These sections contain a number of useful links to templates and model policies, and I want to note that, importantly, they secure the homeland while protecting privacy.

As with you, Madam chair, I do not believe that it is a zero sum game. We can do both, and we can succeed at both or we fail at both. I thank the subcommittee for this opportunity to testify. My office looks forward to working with Assistant Secretary Allen, Dan Sutherland and our fusion center partners to ensure that they maximize their effectiveness by establishing sound privacy practices.

Thank you very much.

[The statement of Mr. Teufel follows:]

PREPARED STATEMENT OF HUGO TEUFEL, III

**Introduction**

Chairman Harman, Ranking Member Reichert, and Members of the Subcommittee, it is an honor to testify before you today on advancing information sharing while safeguarding privacy within the Department of Homeland Security State and Local Fusion Center Program. I am particularly pleased to be appearing with my colleague, Dan Sutherland. As the Subcommittee knows, his office and mine have a statutory responsibility to work together to address privacy as well as civil liberties issues in an integrated and comprehensive manner.

Because this is my first time appearing before the Subcommittee, I would like to introduce myself. I was appointed Chief Privacy Officer of the U.S. Department of Homeland Security by Secretary Michael Chertoff on July 23, 2006. In this capacity and pursuant to Section 222 of the Homeland Security Act of 2002, 6 U.S.C. § 142, my office has primary responsibility for privacy policy at the Department, to include: assuring that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; assuring that the Department complies with fair information practices as set out in the Privacy Act of 1974; conducting privacy impact assessments of proposed rules at the Department; evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government; and preparing an annual report to Congress on the activities of the Department that affect privacy.

I also serve as the Department's Chief Freedom of Information Act (FOIA) Officer. In this role, I assure consistent and appropriate Department-wide statutory compliance and harmonized program and policy implementation. As you know, the three pillars of federal privacy law are the Privacy Act, the Freedom of Information Act, and the E-Government Act.

Prior to joining the Privacy Office, I served as the first Associate General Counsel for General Law at the Department of Homeland Security. Before joining the Department of Homeland Security, I served as the Associate Solicitor for General Law at the Department of the Interior. Therefore, I have had the honor of providing advice and counsel on freedom of information, privacy, and civil rights issues at two cabinet level agencies. As Associate General Counsel for General Law at DHS, Dan and my predecessor as Chief Privacy Officer, Nuala O'Connor Kelly, were my clients, which provided me with the opportunity to understand the issues both offices faced.

There are two other things I should mention. As the Chief Privacy Officer, I currently hold a policy position in the Department, so I limit my practice of law to the weekends, when I serve as a judge advocate in the Army National Guard, within the Legal Support Office, attached to the District of Columbia Army National Guard. Additionally, in my spare time I have been working on a master's degree

in National Security Studies through the Naval War College. My studies have aided me in understanding decision-making in the areas of homeland defense and security.

#### ***The Privacy Office***

I am determined to continue the process of “operationalizing privacy” within the Department and its programs, a phrase described to this Subcommittee by Maureen Cooney, the Acting Chief Privacy Officer before my tenure.

To achieve this, the office forms close relationships with system owners and program managers, along with IT security officials, and senior DHS officials. By placing privacy into the program development and decision-making processes of the Department, we can ensure that DHS not only meets its legal requirements, but stands as a model of how privacy can complement and work with law enforcement and intelligence agencies.

As part of our ongoing operations, our Compliance group works with IT security, budgeting, procurement, and financial professionals Department-wide to complete privacy impact assessments, system of records notices, and other privacy documentation relevant to and required for DHS systems and programs.

Our Office also leverages the considerable experience of our International group to develop and maintain DHS’s privacy policy and practices on issues concerning our foreign partners and allies. These issues range from international compliance measures to data sharing initiatives as well as full treaty negotiation and review.

#### ***Fusion Centers***

State and local authorities have created 42 fusion centers around the country. Fusion centers blend relevant law enforcement and intelligence information analysis and coordinate security measures in order to reduce threats in local communities. They also represent a method for providing first responders with “actionable intelligence”; that is information useful and relevant to the day-to-day mission of state and local law enforcement personnel. As of the end of FY 06, the Department of Homeland Security has provided more than \$380 million to state and local governments in support of these centers.

Intelligence Officers from the Department of Homeland Security Office of Intelligence and Analysis currently work side by side with state and local authorities at twelve fusion centers across the country.

This number is about to grow. On September 12, 2006, Secretary Chertoff told the Senate Committee on Homeland Security and Government Affairs that, “Our goal is to have intelligence and operations personnel at every state and major metropolitan fusion center in the United States, sitting in the same room, sharing and analyzing information and intelligence in real time,” with a “two-way flow [of information], with every level of government pooling intelligence.”

This ramping up of fusion centers and the two-way information flow to accompany it will require additional effort and vigilance to ensure privacy rights are protected. As the DHS Chief Privacy Officer, I will strive to make sure privacy concerns are addressed at the beginning of the process, before information is collected and shared. This process begins, in my opinion, with a proposed fusion center utilizing the Department’s fusion center guidelines.

#### ***Privacy and the Fusion Center Guidelines***

The Global Justice Information Sharing Initiative, the Department of Homeland Security, and the Department of Justice collaboratively developed and in August 2006 issued “Fusion Center Guidelines: Developing and Sharing Information in a New Era.” These guidelines are intended to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination, strengthened partnerships, and improved crime-fighting and anti-terrorism capabilities. The document offers a comprehensive guide to the development and operation of fusion centers, as well as provides useful resources and document templates to facilitate implementation. I believe this is an excellent first step in ensuring fusion centers integrate privacy protection into their actions.

Implementing these fusion center guidelines provides an important first step in applying appropriate privacy protections as required under the “Guidelines to Ensure that the Information Privacy and other Legal Rights of Americans are Protected in Development and use of the Information Sharing Environment”—otherwise known as the ISE Privacy Guidelines—and is a major focus of the ISE Privacy Guidelines Committee (ISE/PGC), of which I am a member. In fact, the ISE/PGC already formed a working group to deal specifically with privacy issues surrounding the exchange of data with state and local entities. Since the fusion centers will be the primary mechanism for federal government information sharing with our state, local and private sector partners, the successful implementation of appropriate pri-

privacy policies will be a critical part of ensuring the success of the Information Sharing Environment.

Privacy concerns and methods of addressing them appear throughout the documents. Fusion Center Guideline 3, for instance, urges the inclusion of a privacy committee in the fusion center governance structure. The purpose of this privacy committee will be to "liaise with community privacy advocacy groups to ensure civil rights and privacy protection." Fusion center governing bodies, moreover, are encouraged in this Guideline to collaborate with the Department of Homeland Security, including the Privacy Office, to establish their operating processes.

Fusion Center Guideline 5 urges fusion center partners to utilize memorandums of understanding (MOUs) to govern interactions between the participants, and commit the parties to the principles and policies of the fusion center. The guideline advises that adherence to privacy and security principles should be specifically addressed within all such MOUs. Where DHS shares personally identifiable information with fusion center partners, the Privacy Office will review and approve a Privacy Impact Assessment that covers the privacy and security controls that the MOU must address.

Fusion Center Guideline 8 is dedicated to promoting meaningful and lawful privacy policies at the fusion centers, and to providing mechanisms ensuring that the centers adhere to these policies. This begins with consideration of the Fair Information Principles which are the worldwide baseline for privacy protection: Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing—consideration of which are also, appropriately, required by the ISE privacy guidelines. The Fusion Center Guidelines provide a useful list of complementary elements for the drafters of the privacy policy, including:

1. Add introductory language that clearly states the privacy practices of the center;
2. Describe the information collected and how the information is stored;
3. Establish a common lexicon of terms for dealing with role-based access;
4. Define and publish how the information will be used;
5. Draft a clear, prominent, and understandable policy;
6. Display the privacy policy for both center personnel and customers;
7. Ensure that all other policies and internal controls are consistent with the privacy policy;
8. Establish a business practice of notifying government agencies of suspected inaccurate data;
9. Adhere to applicable state and federal constitutional and statutory civil rights provisions;
10. Partner with training centers on privacy protection requirements and conduct periodic privacy security audits;
11. Consult with the privacy committee (established pursuant to Guideline 3) to ensure that citizens' privacy and civil rights are protected;
12. When utilizing commercially available databases, ensure that usage is for official business and the information is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data; and
13. Determine if there are security breach notification laws within the jurisdiction and follow those laws, if applicable.

Having defined the key elements of a sound privacy policy, the rest of Guideline 8 focuses on the steps the leaders of the fusion center should take to ensure the policy is followed. These steps include such prudent steps as ensuring adequate training and information privacy awareness and establishing a policy for tracking and reviewing privacy complaints and concerns. Guideline 8 also recommends seeking legal counsel. I would only add to this list that participants should also consult frequently with their entity's Chief Privacy Officer.

The supplemental materials available on the Guidelines' companion CD are particularly useful. They include the Justice Department's *Privacy and Civil Rights Policy Templates for Justice Information Systems*, Privacy Policy Templates, and a Privacy Policy Development Guide.

The *Privacy Policy Development Guide* recommends that in addition to the development of a comprehensive privacy policy, fusion centers complete privacy impact assessments to understand the effect that technology and operation choices have on privacy. The Privacy Office developed a detailed methodology to analyze the impact any new or update system will have on an individual's personal information, including reviewing:

- What information is to be collected;
- How will be it stored, managed, and used;

- What means of individual access is available;
- What means of redress for informational errors has been provided; and
- What security is in place to protect the information.

The Privacy Office's official guidance on the writing of privacy impact assessments to shepherd the different system programs safely through the privacy protection process serves as an appropriate addendum to the Fusion Center Guidelines.

Furthermore, it is often said that "security concerns become privacy problems." Privacy protection principles are only meaningful if they exist in tandem with a robust security regime. Fusion Center Guideline 9 provides a framework for ensuring adequate security measures are in place. This includes, of course, security for facilities, data, and personnel. A fusion center's Privacy Officer and Civil Rights Officer must have close working relationships with its Chief Information Officer as well as the Chief Security Officer.

As a whole, I believe these guidelines provide an invaluable resource for the principals to utilize when founding and operating a fusion center, and will also be helpful to me, as a member of the ISE Privacy Guidelines Committee, in monitoring how privacy is safeguarded in this crucial aspect of the Information Sharing Environment. The Fusion Center Guidelines encourage consideration of privacy interests from the very moment of formation—a critical step.

#### ***Privacy Office's Review of the MATRIX Program***

Information sharing, of course, is at the heart of fusion center activities. The Privacy Office has had an opportunity to review a pilot information sharing program among a number of state governments called MATRIX, the Multistate Anti-Terrorism Information Exchange. The program accessed only state-owned or publicly available records that were already available to law enforcement without a subpoena or court order. DHS became involved in the pilot in July 2003, when (what is now) Grants and Training entered a Cooperative Agreement with a non-profit entity to administer the project. The funding was intended to assist with testing the system for data analysis and integration of terrorist threats and other intelligence information, as well as to provide funding to establish user accounts for MATRIX participants and to create a secure website for each participating state to facilitate information sharing.

The Privacy Office reviewed the program following a request by the American Civil Liberties Union and published its findings in a report entitled, "Matrix Report—DHS Privacy Office Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project," which is available on the Privacy Office website.

We found that the project lacked a privacy policy that clearly articulated the project's purpose, how it would use personal information, the types of information covered, and the security and auditing safeguards governing the project. The MATRIX Board of Directors did not issue a privacy policy of any kind until four months after the pilot began. It was nearly a year before the Board approved an audit requirement and then it merely called for a self audit.

The Privacy Office believes, however, that the MATRIX pilot project was undermined, and ultimately halted, in large part because it did not have a comprehensive privacy policy from the outset to provide transparency about the project's purpose and practices and protect against mission creep or abuse. The recommendations of the Privacy Office rest on the basic premise that information programs such as the MATRIX pilot project can protect privacy, while securing the homeland. Building privacy into the architecture of an information program can help ensure that such programs achieve their objectives while at the same time safeguarding individual privacy. This is more than just a compliance issue. The Privacy Office understands that sound and effective privacy practices maximize the utility of the information collected, processed, and maintained by DHS to facilitate and improve performance, while minimizing the cost to agencies and to the public.

I note that the MATRIX program was initiated and failed before the fusion center guidelines were issued. If the MATRIX participants had had the benefit of these guidelines and followed their plan for implementation and the creation of a comprehensive privacy policy, I am confident that the program would have stood a much better chance of success. Looking forward, I hope parties entering future information sharing agreements, especially in support of fusion centers, read the MATRIX report for its lessons learned and then review and adopt the Fusion Center Guidelines. And of course they should consult their Privacy Office.

#### ***Conclusion***

I thank the Subcommittee for this opportunity to testify. My office looks forward to working with the Department and our fusion center partners to ensure they maximize their effectiveness by establishing sound privacy practices.



I look forward to hearing my colleagues' testimony and to answering your questions.

Ms. HARMAN. Thank you for your testimony within the time limit. A vote has been called. I am not sure if it is the last vote, but we have about 10 good minutes. It is not the last vote. So I think we will try to conclude this hearing before we go to vote. I think that is fairer to you and would work better.

Ms. HARMAN. So I am going to just make a comment as to one question, and take less than 5 minutes and then yield to the other two that are here. My comment is that you have revealed a closely guarded secret. Folks out in the countryside don't realize that you are there and what you are doing, and I would urge you to tell your story. In fact, I would urge committee staff to figure out the way we are going to tell this story in Los Angeles on April 5 because it is very important that the neighborhoods which these fusion centers serve understand that this training is available and conducted and that the policies that these fusion centers are following hopefully comply with these Federal policies. And so my one question is, maybe Mr. Sutherland for you if you could answer it in 30 seconds, and then I will go to Mr. Reichert. Can you assure me that people who are coming now to the JRIC, the Joint Regional Intelligence Center, in Los Angeles, receive this training, watch your video, read your materials and practice these guidelines that you have developed?

Mr. SUTHERLAND. Chairwoman, I could not assure you that any particular employees of any particular fusion center have seen this video or seen these materials that I referenced. We need to do a better job in that regard.

Ms. HARMAN. Well, then, let me just conclude by urging you to do a better job in this regard and find the ways to make these programs known by those who work in these fusion centers. We are, by legislation, considering making some of this mandatory if, as Charlie Allen says, everyone wants to follow these practices, and that can be done even before they are mandatory. Let's do that. Would you commit to working on that problem?

Mr. SUTHERLAND. Absolutely. We will do it, and we will follow up with you.

Mr. DICKS. If I could just add—

Ms. HARMAN. Yes. I will yield to you.

Mr. DICKS. Do you have a plan to do this?

Mr. SUTHERLAND. Not specifically with regard to fusion centers. We have, for example, the training that I mentioned on Arab Muslim values and culture, we have just had that out for a month, and 4,000 copies are gone. We have a tremendous amount of enthusiasm. So we are confident that when we make this available to individuals in fusion centers, that they will take it. We have distributed over 600 at the training last week, but I think we can definitely follow up to contact them directly and say, here is what we have available.

Ms. HARMAN. Well, I think Mr. Dicks raises exactly the right point. We are all late in this, our understanding of Muslim and Sikh and other cultures is lagging in America. And to make policies to protect our homeland work, we obviously have to have better understanding and hopefully gain the trust of law-abiding citizens

from all these communities who are the first to know whether something is wrong in their neighborhoods, and we want them to tell us if something is wrong. So let us urge you to think through quickly how this information can go out to fusion center personnel, what steps we might have to take to help you get there. Obviously, we are talking about additional budget resources. But let me put that out and follow up with you within a week or so to see where we are, and maybe you can report back on April 5 or someone can in Los Angeles. Is that reasonable?

Mr. SUTHERLAND. Yes, ma'am.

Ms. HARMAN. Thank you. Let me yield a few minutes to Mr. Reichert and then to Mr. Dicks.

Mr. REICHERT. Thank you, Madam Chair. And I think you make an excellent point and follow it up by Mr. Dicks. And as you were both speaking, I jotted down some quick notes and it just so happens that my questions for both of you are along the same lines as we have just experienced here. So you, Mr. Sutherland, mentioned that the Secretary made a comment at the fusion center conference that there are tools and measures in place to safeguard—they wanted to make sure there were tools and measures in place to safeguard privacy and civil liberties, and certainly education has got to be at the top of the list. And then, Mr. Teufel, you mentioned the assistant secretary, his comment was sound and effective policies. What tools and measures or policies are you talking about? Just kind of bullet point them real quick for me, please.

Mr. TEUFEL. Well, I would call your attention to the guidelines and it is—I am going to get this wrong—the fusion center guidelines. But Section 8, title 8, deals with the privacy guidelines. Now, it is true that under the guidelines, these privacy requirements are not mandatory, but they are recommended. It is my understanding in talking with the folks over at INA that INA looks to make sure that the privacy guidelines are implemented before they send folks out. And I want to stress that these privacy guidelines contained in the fusion center guidelines are outstanding, and key to them—at the heart of them are the fair information practice principles that undergird the Privacy Act of 1974, the eight fair information practice principles. And if you adhere to those principles, you can't go wrong when it comes—

Ms. HARMAN. Mr. Reichert, would you yield to me just for a request of the witness? Would you provide that material for us, please? I am assuming it is unclassified, but whatever form it is in, we would like to receive it.

Mr. TEUFEL. Absolutely, ma'am. We pulled it down off the Internet yesterday. It is publicly available, and we can certainly get to you.

Ms. HARMAN. Mr. Reichert. I would point out we are at about 8 minutes, so hopefully we can get to Mr. Dicks.

Mr. REICHERT. The tools and measures are the same as the policies? We are talking about the same thing?

Mr. SUTHERLAND. Yes, Congressman. I think one thing that is important when you look at the guidelines is that the guidelines, most of the discussion in this context deals with the protection of data which falls within Mr. Teufel's area. The sorts of training that I was talking about would fall more in the area of the protection

of civil rights or a better understanding of what to do with data, and that is I think where we can really add value here.

Ms. HARMAN. Mr. Dicks you have 2 minutes for questions.

Mr. DICKS. So you have ways of—when people gather information, which is what this is all about, you have got ways of protecting the databases and protecting that information. Is that correct? Or is that something you will have to work on and develop in each one of these fusion centers?

Mr. TEUFEL. Well, every fusion center is different. They are established by State and local governmental entities. The Department of Homeland Security and the Department of Justice participate alongside as partners. If I understand—

Mr. DICKS. Let's say they get—you know, we are sending top secret information back and forth. I mean, they have got to have some way to protect that information at the, say in the Los Angeles center or the Seattle center.

Mr. TEUFEL. Absolutely, sir. And when it comes to the transmission of classified information, there are protocols in place and standards that have to be met. I think it is important to note that you can have all the great gear in the world, all the best technology in the world, and you can still fail because as long as there are human beings involved, human beings will make mistakes. And so the answer is always training, training, training, training, so that people do the right thing.

Mr. DICKS. And good judgment.

Mr. TEUFEL. Yes, absolutely.

Mr. DICKS. And knowing the rules.

Mr. TEUFEL. Hopefully, we don't hire people that don't have good judgment or who don't know the rules.

Mr. DICKS. One point, as we walk out the door, it sounds like we are having—a lot of people are coming to the fusion center, and each situation is different. So you know, is there a way—are these people cleared? Do we look into their records? Is there a clearance process of sorts before these people become part of the fusion center?

Mr. TEUFEL. That is my understanding, sir. And as I also understand, INA looks at the people and looks at the centers before they get involved, sir.

Ms. HARMAN. Let me thank both of our witnesses. As Mr. Allen said about fusion centers, one size does not fit all, but what has to fit all is that civil liberties and privacy principles are observed all the time. No exceptions. And it is going to be hard to get this right, training training, training, is clearly a big part of the answer, and I just want to commend both of you for what appears to me to be excellent work at the Department of Homeland Security. The hearing stands adjourned.

[Whereupon, at 4:42 p.m., the subcommittee was adjourned.]

#### PREPARED STATEMENT OF HON. BENNIE G. THOMPSON

Thank you, Madame Chair, and I join you in welcoming Mr. Allen, Mr. Teufel (pronounced "Too-ful") and Mr. Sutherland to this important hearing on State and local fusion centers.

The central role that fusion centers are and should be playing in improving information sharing cannot be overstated. The Department must work together with its law enforcement, first responders, and private sector partners at the State and local

levels if we are ever to have truly safer homeland. They are often in the best position to know what their information needs are what intelligence would be most useful to them for figuring out where to spend their resources. That's what intelligence is all about: if it can't tell us what to prepare for and how, what good is it?

Fusion centers were launched by State and local leaders themselves to get a handle on these and other issues, and I commend your office, Mr. Allen, for the "customer service" approach it has taken in this regard. That approach strikes the right balance between showing respect for the hard work that the States and locals already have done with fusion centers while at the same time showing how the Department can help them going forward.

But we can't help you help the fusion centers, Mr. Allen, if we don't know what you need. I hope you'll be forthcoming about the challenges ahead for your State and Local Fusion Center Program given the President's Fiscal Year 2008 budget request. I hope you'll also be able to give us a sense of where you plan to deploy your resources as part of that Program.

Mississippi is in the process of planning a fusion center, and I imagine it could have played a key role in saving lives in the wake of Hurricane Katrina. How your Program will help improve situational awareness in the Gulf Region is of great interest to me.

Moreover, I agree wholeheartedly with Ms. Harman that fusion centers must keep the faith with the American people. Privacy and civil liberties must be a centerpiece of the Department's efforts at State and local fusion centers. I hope you'll address what you're already doing on this front, and that you'll share your thoughts on how to promote a rigorous defense of privacy and civil liberties at these centers.

I encourage you to work closely with Mr. Teufel (pronounced "Too-ful") and Mr. Sutherland about how to incorporate a training regimen as part of your efforts. I am certain that they are full of good ideas about how to do that.

Thank you again, and I look forward to your testimony.

#### ADDITIONAL QUESTIONS AND RESPONSES

##### QUESTIONS FROM HON. BENNIE G. THOMPSON

##### RESPONSES FROM HUGO TEUFEL AND DANIEL W. SUTHERLAND

**Question 1:** In our efforts to secure the homeland, information sharing efforts at State and local fusion centers are becoming increasingly important to create the kind of situational awareness that is necessary to prevent the next terrorist attack. While we want to defeat the terrorists, we don't want to destroy our Constitutional rights in the process. I'm very interested in learning more about how Mr. Allen's State and Local Fusion Center Program could be a catalyst for protecting these rights.

**How might the Privacy Office and Office for Civil Rights and Civil Liberties partner to create a privacy and civil liberties curriculum that could be taught to staff at State and local fusion centers, and what might that curriculum look like?**

**To what extent are your offices equipped to provide privacy and civil liberties training to Department and other staff at State and local fusion centers, and what would such a training program cost in your estimation? How long would it take you to put such a training program together?**

**Answer:** Section 222(5)(A) of the Homeland Security Act of 2002 requires the Chief Privacy Officer to coordinate with the Officer for Civil Rights and Civil Liberties on programs, policies and procedures involving civil rights and privacy. Currently, in connection with the Information Sharing Environment Implementation Plan, the Privacy Office and the Office of Civil Rights and Civil Liberties coordinate efforts to build appropriate protections for privacy and civil rights into the fabric of the Information Sharing Environment. Were Congress to enact legislation requiring training for staff of State and local fusion centers, I am confident that the Privacy Office and the Office of Civil Rights and Civil Liberties could partner to create an effective training program.

With respect to the privacy aspect of such training, the privacy curriculum would focus on creating a culture of awareness within fusion centers that respects privacy interests of individuals. Such a curriculum would introduce the three pillars of federal privacy law: the Privacy Act of 1974, the Freedom of Information Act, and the E-Government of 2002. In addition to federal authorities, the training should acknowledge individual state privacy laws that govern the operation of fusion centers. The State and local fusion centers are creations of the individual States and hence

are subject to their own statutory and constitutional requirements to protect the rights of their citizens.

The training would include a thorough examination of the Fair Information Principles (FIPs) reflected in the Privacy Act with the enhancements made by the Privacy Office to encompass the full breadth and diversity of the collection, use, dissemination, and maintenance of personally identifiable information (PII) at the Department. The Privacy Office's Fair Information Principles are Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

The curriculum would review how the Privacy Impact Assessment (PIA) process applies these FIPs to specific program requirements to aid fusion center staff in identifying and mitigating privacy challenges.

Next, the curriculum would introduce the President's Information Sharing Guidelines, which encourages the Federal government to share information with State and local partners while respecting and protecting privacy. ISE Privacy Guidelines outline the specific process for the protection of privacy and other rights. In addition, the training would introduce fusion centers to the requirements of 28 CFR Part 23, which provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and the review-and-purge process. The training would encourage fusion center staff to avail themselves of additional training offered on this regulation.

Finally, the training would refer the staff of fusion centers to the Fusion Center Guidelines document developed collaboratively by the Global Justice Information Sharing Initiative, the Department of Justice, and the Department of Homeland Security. These Guidelines are intended to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination, strengthened partnerships, and improved crime-fighting and anti-terrorism capabilities. The document offers a comprehensive guide to the development and operation of fusion centers, including information on privacy and civil liberties protections, and provides useful resources and document templates to facilitate implementation. A number of its recommendations and resources explicitly address enhancements to privacy protections. This is an excellent first step in ensuring fusion centers integrate privacy protection into their actions.

To create a curriculum to embed privacy into the development and operations of fusion centers, the Privacy Office would revise and augment its existing training modules for Privacy Awareness, Privacy Act 101, and Privacy Act 201, the PIA guidance, and the Fusion Center Guidelines into an e-learning course specifically addressing the privacy issues surrounding a multi-party, multi-jurisdictional fusion center. Based on previous privacy course development efforts, the Privacy Office estimates that this effort could take six to nine months to develop and cost approximately \$250,000, which would include course development support for the Privacy Office, but would not include the resources necessary to deploy the training across existing and developing fusion centers.

**Question 2.:** I would imagine that some State and local fusion centers will be more open to a Department-sponsored privacy and civil liberties training program than others. Some may already have similar programs in place, while still others simply may not see the value of such training.

**What kind of incentives would be helpful, in your view, to encourage State and local participation in any privacy and civil liberties education program that the Department might offer?**

**Answer:** The benefits of implementing robust privacy programs into fusion centers are manifest. They help ensure public confidence and enhance rather than erode fusion center performance. In recognition of this, Fusion Center Guideline Number 8 encourages prudent measures to foster respect for privacy including adequate training and information privacy awareness.

Although developing specialized training provides efficiencies regarding the incorporation of privacy protections into the development and operation of fusion centers, the Fusion Center Guideline Number 5 urges the utilization of memoranda of understanding (MOU) between fusion center partners that helps define privacy responsibilities. These MOUs could establish requirements for fusion center staff to receive periodic privacy training developed in a collaborative environment and integrating any training from the Privacy Office.

**Question 2.:** Given the increasing public focus on State and local fusion centers, what risks may arise if such centers fail to get privacy and civil liberties "right"?

**How might an aggressive privacy and civil liberties training program help build public confidence in fusion centers?**

**Answer:** Getting privacy “right” is more than just a compliance issue—it is vital to the success of every fusion center. A comprehensive privacy policy will help staff understand what information they will use and why. This will frame their activities to ensure they stay on mission.

Failure to respect privacy will jeopardize fusion center effectiveness and will erode public confidence. The Privacy Office’s report on the MATRIX program discussed in my March 14 testimony bears this out. The information sharing relationship between several states in MATRIX failed amid public concern because it lacked a privacy policy that clearly articulated the project’s purpose, how it would use personal information, the types of information covered, and the security and auditing safeguards governing the project.

Any effective training on privacy and civil liberties issues requires close coordination between my office and Civil Rights and Civil Liberties. That cooperation exists presently.

We believe privacy training can help fusion centers to avoid the fate of MATRIX in two ways. First, it can provide a sound basis for understanding general privacy principles through the FIPs and learning how to adhere to federal and state privacy laws. In addition, it can demonstrate to DHS’s fusion center partners the importance the Department places in privacy.

Fusion center training can also help establish public confidence in the program. Guideline 3 of the Fusion Center Guidelines addresses governance issues and recommends creating a privacy committee to interface with community privacy organizations. The completion of privacy training for fusion center staff is one of the measures that leadership can point to when demonstrating their commitment to preserving privacy rights.

**Question 4:** Fusion centers are spreading all over the country, and the Departments of Homeland Security and Justice are both offering more and more resources to encourage their development.

**In your view, what are the risks to privacy and civil liberties at State and local fusion centers, and what resources should the Federal Government be offering to fusion centers to avoid those pitfalls?**

**Answer:** In my answer, I will focus on privacy issues and I defer to my colleague, Dan Sutherland, on the civil liberties implications. Privacy problems occur when programs like fusion centers do not define a solid privacy framework to help adhere to the FIPs. Without a privacy framework in place, a fusion center runs the risk of over-collecting information, disseminating information too broadly, applying inadequate security controls, and encouraging any number of other privacy, and civil liberties, problems.

As I stated in my March 14 testimony and throughout these questions, the Fusion Center Guidelines issued by the Global Justice Information Sharing Initiative, provide a wealth of information and practical resources for establishing and running a fusion center.

Guideline 3 encourages a governance structure which includes a privacy committee; Guideline 5 urges the use of MOUs which include privacy policies and responsibilities; Guideline 8 deals entirely with privacy and civil liberties; and Guideline 9 provides recommendations which help prevent security weaknesses from becoming privacy problems.

Adherence to these guidelines and development of the training and policies they recommend are critical steps in ensuring that the fusion centers provide the maximum benefit to the nation, without minimizing privacy rights and thus losing the confidence of the public that the fusion centers are in business to protect.

**Question 5:** What privacy and civil liberties “best practices” would you most like to see adopted at State and local fusion centers and why?

**How might an “in-person” training program offered by the Department of Homeland Security at State and local fusion centers encourage adherence to these best practices?**

**Answer:** The Privacy Office believes every fusion center should have an official responsible for privacy issues. This official could ensure that the best practices described in the Fusion Center Guidelines are implemented appropriately and that compliance issues are dealt with in a timely manner. Among these best practices are: adherence to the FIPs; periodic privacy audits; adequate security controls; and regular interaction with the public and privacy advocacy groups.

In-person training can help define these best practices for fusion center staff and refer them to the planning and implementation resources available within the Fusion Center Guidelines. Again, I defer to my colleague from CRCL on the civil liberties implications.

**Question 6.:** There is a lot of mystery surrounding fusion centers. Recent press accounts report that some privacy and civil liberties advocates fear that they might become domestic intelligence agencies that spy on Americans. Others worry that a lack of familiarity with privacy and civil liberties laws and regulations raise the risk of accidental—but equally damaging—breaches of Constitutional rights.

**What checks are in place at fusion centers that, in your view, might help them avoid becoming mini spy agencies, and where might there be a need for greater oversight to ensure that abuses don't occur?**

**Answer:** First and foremost, fusion centers are analytical, not operational, entities. They access existing information and analyze it. As well, they aid Federal, State, and local entities in finding information. Fusion centers do not independently gather information.

Second, transparency in implementing the FIPs is critical to keeping a fusion center focused on its lawfully authorized information sharing mission. A public airing of its practices for the collection, use, dissemination, and maintenance of personally identifiable information will benefit the operation of the fusion center in two important ways. It will provide discernable limits on the actions of fusion center staff. As well, it will help the public understand the important but focused purpose of the fusion center. With this understanding they will be less likely to fear the creation of a mini spy agency in their midst.

Third, a fusion center can conduct periodic audits to confirm staff is adhering to the purpose and limits originally defined. Moreover, the transparency of the initial privacy assessment can be regularly buttressed by liaising with members of the local community and interested privacy advocacy groups.

**Question 7.:** What privacy, civil liberties, and data security training do your offices provide to DHS employees being deployed to State and local fusion centers, how is that training given, and how often are DHS staff required to undergo refresher courses?

**In your view, to what extent is the training that your offices provide to DHS employees transferable to State, local, and tribal personnel at State and local fusion centers?**

**Answer:** Currently, every new employee hired by DHS receives an introduction to the Privacy Office and the three pillars of federal privacy law: the E-Government Act, the Privacy Act, and the Freedom of Information Act.

In addition to the new employee orientation, the Privacy Office has developed and distributed an e-learning privacy training course entitled "Privacy Awareness," which expands upon the basic concepts presented in the orientation to develop an understanding in the essentials of the Privacy Act and E-Government Act. This training permits DHS employees and contractors to recognize situations in which privacy issues arise and how best to mitigate risks to privacy in the development and operation of a program. This course is available across DHS and has been or will soon be incorporated into the various training programs. The Privacy Office is nearing the completion of the development of two Privacy Act e-learning courses entitled "Privacy Act 101" and "Privacy Act 201." The initial one-hour course, "Privacy Act 101," will provide all employees and contractors with the essentials concerning the Privacy Act of 1974, including a basic understanding of what is personally identifiable information, what is a system of records, when is a System of Records Notice required, how can information be collected, used, maintained, or disseminated in compliance with the Privacy Act, and other related topics. Further, it introduces DHS employees and contractors to the Fair Information Principles employed by the Privacy Office. Once all the courses are completed, they will be used as annual refresher courses to ensure a complete understanding of privacy issues facing the Department.

As already discussed, with modest changes, these privacy courses could form the core of a training curriculum to support fusion center staff. They cover federal privacy law as well as the FIPs in detail. Adherence to these is critical for fusion centers to accomplish their mission without eroding privacy rights.

Nonetheless, these existing DHS modules are just the beginning. Fusion center training, in particular, should add specific references to the invaluable Fusion Center Guidelines and, where possible, such training should contain information on relevant state privacy law as well.

All personnel employed by or assigned to the Office of Intelligence and Analysis (I&A) are **required** to attend Intelligence Oversight and Information Handling on an annual basis. This training is required **wherever** the I&A employee is assigned, to include those working in the State and Local Fusion Centers. This Intelligence Oversight and Information Handling training addresses the proper handling of information which identifies United States (US) persons, such as social security num-

bers. The training emphasizes that I&A personnel must be familiar with I&A's mission, and the proper method of collection, retention, and dissemination of information about US persons. Part of this training includes a review of the history of past abuses of these rights.

**Question 8.: What should a model privacy and civil liberties education program include as part of its core curriculum?**

**What would be the most important thing for law enforcement and other staff at fusion centers to know about privacy and civil liberties as they do their fusion work?**

**Answer:** As noted above, the privacy curriculum would focus on creating a culture within fusion centers that respects privacy interests of individuals. It would begin with an introduction of the three pillars of federal privacy law: the Privacy Act of 1974, the Freedom of Information Act, and the E-Government of 2002. It would include an introduction to the Information Sharing Environment Guidelines, including the ISE Privacy Guidelines, as well as to 28 CFR Part 23. The training would note that, in addition to these Federal laws and regulations, individual state privacy laws may govern the operation of individual fusion centers as well.

The training would include a thorough examination of the FIPs including Openness, Individual Participation, Purpose Specification, Minimalization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. Additionally, the training would demonstrate how DHS uses PIAs to evaluate a program using these FIPs. Finally, the training would refer the staff to the Fusion Center Guidelines to address fusion center specific issues.

In addition to this training, law enforcement and other staff at fusion centers should understand that adherence to privacy law and application of the FIPs is not just a compliance issue. It is the best method of assuring information at their disposal is utilized effectively. Moreover, a transparent respect for privacy is critical for maintaining the confidence of the public they are trying to serve. Without this confidence, there is a chance their program will cease to exist or not have access to critical citizen-borne information.

**Question 9.:** One civil liberties concern at fusion centers involves data integrity—how safe is information in fusion center databases from being hacked or otherwise accessed by people with no right to it.

**What should a privacy and civil liberties curriculum include to address the data integrity issue? What best practices would you recommend?**

**Answer:** While state privacy law will govern the operation of fusion centers, the documentation of these procedures in documents similar to the Privacy Impact Assessment and System of Records Notice required of federal agencies, as well as developing and implementing records retention schedules, provides invaluable insight into information collection, use, dissemination, and maintenance policies and procedures of the fusion center.

A privacy curriculum would stress that data integrity is a matter of primary concern. From a privacy perspective, information assurance is crucial for any program deploying information technology handling the exchange of data between multiple participants. The Privacy Office FIPs include three principles that go to the heart of data integrity: Data Quality and Integrity, Security, and Accountability and Auditing.

The first, Data Quality and Integrity, looks to ensure that personally identifiable information is accurate, complete and kept up-to-date. Under this principle, the fusion center training would encourage regular review of personally identifiable information to ensure it remains relevant and necessary to the purposes of the program or an investigation. Once personally identifiable information is no longer relevant and necessary, the information should be purged from the supporting systems. To accomplish these goals, fusion centers should have standard operating procedures outlining how to review information for relevant and necessary standards. These procedures should be documented in the Privacy Impact Assessment and System of Records Notice as well as developing and implementing records retention schedules.

The second principle, Security, looks to protect personally identifiable information through reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure. This principle is implemented through appropriate information security controls, such as required through the Certification and Accreditation process outlined by the Federal Information Security Management Act (FISMA) and the DHS Chief Information Security Officer (CISO).

The third principle of this list, Accountability and Auditing, looks to hold the fusion center and its participants accountable for complying with measures which give effect to all the principles. The fusion center should develop mechanisms to ensure ongoing compliance with these fair information principles. Technology should sup-



port the ability to perform appropriate audits to measure up operational metric with privacy protections. Further, for information from federal partners, DHS should provide appropriate training to all employees and contractors that handle personally identifiable information.

**Question 10.: If both your offices work together, how long would it take you to develop a privacy and civil liberties training program, and what steps have you considered already for establishing and implementing such a program?**

**What kind of resources will your offices need to help you establish and implement a fusion center-oriented privacy and civil liberties training program in a timely fashion?**

**Answer:** At present, the office has sufficient appropriations only to carry out its presently-assigned mission. As I have detailed earlier, the Privacy Office training courses, including Privacy Awareness, Privacy Act 101, and Privacy Act 201; the DHS Privacy Impact Assessment Guidance; and the Global Fusion Center Guidelines would serve as the basis for any training created for fusion centers. It would take between six and nine months to accomplish this.

While the manner of training delivery is yet to be determined, one scenario for properly deploying a fully-functional privacy training program to federal participants and fusion center operators in a timely manner will require funding for both personnel and development support. Having a team from the Privacy Office dedicated to providing training to fusion centers is the first step. Optimally, hiring or contracting for a fusion center privacy training coordinator and an appropriate number of trainers to go out to the fusion centers and provide ongoing instruction in privacy issues would provide the quickest and most effective approach to ensuring privacy protections in the deployment and operation of fusion centers.

In addition to training resources, privacy resource support will be necessary to ensure that the training received by fusion center participants is properly employed through the development of privacy policies and compliance programs at the individual centers. Dedicating personnel at the Privacy Office to support this effort would ensure uniformity throughout the various fusion centers in the application of the FIPs to protect privacy. I anticipate that we would need an additional compliance specialist within the Privacy Office.

#### RESPONSES FROM DANIEL W. SUTHERLAND

**Question 11.: In your view, Mr. Sutherland, would it be appropriate for DHS to offer a standardized privacy and civil liberties training program to State and local fusion centers where DHS has a presence?**

**What benefits might derive from such a standardized approach? To what extent would a fusion center-oriented privacy and civil liberties training program need to vary from State to State according to the needs of each location?**

**Answer:** In my answer and in responses to subsequent Questions for the Record, I will focus on Civil Rights and Civil Liberties aspects, and defer to my colleague, Hugo Teufel on the privacy implications.

First let me state that it is important to remember that fusion centers were created and are run by State and local officials and not the Federal government. Yes, CRCL could offer a standardized program detailing the framework within which all fusion centers with a DHS presence should operate. Such a standard program would likely cover only those systems, approaches, policies and missions that are nearly universal for fusion centers. A standard program would help create a baseline expectation for what knowledge all personnel should have in order to conduct their work in fusion centers. This would be a voluntary program for non-DHS employees not connected to a DHS program or grant.

Variation would depend on many factors including the type of information shared, the variety of systems and architecture used to control and share information, the level of cooperation, the volume of work to be conducted and the track record of individual fusion centers.

**Question 12.: Mr. Sutherland, if you were to develop a privacy and civil liberties curriculum for State and local fusion centers, what procedures would you have in place to make certain that racial profiling does not exist within the fusion center context and how will you address racial profiling in the training program?**

**Answer:** In June of 2004, the Department issued a memo to all staff describing its policy on racial profiling, and adopting the latest Department of Justice policy on profiling, itself issued in June of 2003. CRCL has created training on racial

profiling that is at least applicable to Federal activities undertaken using information obtained and shared through fusion centers, if not to the activities of State and local law enforcement entities themselves.

Training fusion centers on racial profiling would provide an opportunity to offset some of the risks associated with information overload. Large quantities of raw information provided to State and local agencies without analysis or assurance of reliability can lead to assumptions that may be at odds with equal protection standards and, in the extreme, result in racial and ethnic profiling. Fusion centers, through their approach to cooperative analysis, can provide information that is reliable and concrete enough to eliminate the uncertainty that can lead to racial and ethnic profiling. Further, basic cultural competence training can better enable fusion center partners to, in turn, equip their personnel with knowledge that will help them do their jobs in a manner that shows respect to, and earns the respect of, the communities they protect and serve.

**Question 13.: Mr. Sutherland, how would you ensure that your office continues to serve as a resource to fusion center personnel after any privacy and civil liberties training you provide is complete?**

**Answer:** We will ensure that CRCL continues to serve as a resource to fusion center personnel by being responsive to follow-up questions and by establishing ongoing dialogue with fusion center personnel. We will work with DHS I&A, the DHS Information Sharing Coordinating Council and Governance Board, the Information Sharing Environment Program Manager and others involved in the information sharing environment to voice civil rights and civil liberties concerns at all stages of Federal planning and policy making related to fusion centers. Where appropriate, we will continue to serve as a resource by making our training material available to criminal justice programs and other institutions that provide training to fusion center personnel. The Office for Civil Rights and Civil Liberties will use its available resources to provide assistance to fusion centers across the country so that they can fulfill their mission at the highest level of effectiveness.

**Question 14.: Notwithstanding the support provided to the fusion centers from your office, Mr. Sutherland, would you support fusion centers having an individual on-site to provide on-the-spot civil rights and civil liberties advice to employees when circumstances warrant?**

**Why or why not? How might your office encourage that fusion centers have such a person on staff?**

**Answer:** Depending on the size and mandate or mission of the fusion center it may or may not be useful to have an individual on-call or on-site to provide immediate civil rights and civil liberties advice. A large, regional fusion center with scores of government partners will likely have more circumstances that warrant daily seeking expert civil rights and civil liberties advice. Even in such instances there is a great deal that could be accomplished using secure networks in an on-call approach.

The Office for Civil Rights and Civil Liberties is one of the smallest such offices in the federal government. For sake of comparison, the Department of Justice's Civil Rights Division has approximately 800 employees and the Department of Education's Office for Civil Rights has approximately 600 employees. Because of the size of its workforce, for example, the Department of Education is able to staff regional offices around the country. The Office for Civil Rights and Civil Liberties has approximately forty full-time employees. Given this, we recognize that we must spread our influence through innovative projects such as Civil Liberties University, our training vehicle. We continue to look for ways to share our expertise with our colleagues around the country.

**Question 15.: Mr. Sutherland, I'm aware that your office has prepared training courses for DHS staff that is available on CD-Roms and other media. For purposes of a fusion center-oriented privacy and civil liberties training program, what portion of the training should be "in person" versus on CD-Roms or other media?**

**What role could community outreach from fusion centers play in reinforcing the privacy and civil liberties lessons you might teach?**

**Answer:** Again, I will focus on Civil Rights and Civil Liberties issues and I defer to my colleague, Hugo Teufel on the privacy implications.

As much as possible, a standardized tool should be used in order to save resources and ensure widespread access to the training. Where circumstances warrant "in person" training, CRCL, working with our partners in the Privacy Office, will be able to provide such training and may be able to tailor it to specific fusion centers, depending on the circumstances on individual fusion centers and assuming sufficient

resources are available. Effective training is ordinarily developed in response to various types of needs analysis, and any training provided under such a program should be designed in the method most likely to ensure effective delivery of the curriculum.

I would encourage Fusion centers to actively engage communities to ensure widespread understanding of their mission, capabilities, and their efforts to ensure privacy and civil liberties principles are respected. Disclosure of the privacy and civil liberties guidelines, policies and training will help to create community support. Affording the public ample opportunities to express concerns and raise questions will foster trust that leads to cooperation in the activities undertaken by all fusion center partners.

#### RESPONSES FROM HUGO TEUFEL

**Question 11.:** Mr. Teufel, some states have applied for exemptions from the Privacy Act to expand the amount of information they can collect and retain at fusion centers.

**What concerns does this raise for you, and how do we go about ensuring that fusion centers do not eviscerate the Privacy Act?**

**Answer:** The Privacy Act of 1974 applies only to federal agencies; it does not govern the actions of the states in connection with fusion centers. Nonetheless, although the Privacy Act of 1974 permits Federal agencies to control access to information held in a Privacy Act System of Records (SOR), such exemptions do not remove all of the requirements of the Privacy Act. Typically, Federal agencies will promulgate a rule to exempt a particular SOR from certain sections of the Privacy Act.

Federal agencies need these exemptions in order to protect information relating to law enforcement investigations from disclosure to subjects of investigations and others who could interfere with investigatory and law enforcement activities. Specifically, the exemptions are required to preclude subjects of investigations from frustrating the investigative process; to avoid disclosure of investigative techniques; to protect the identities and physical safety of confidential informants and of law enforcement personnel; to ensure Federal agencies' ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard sensitive information.

Importantly, the exemption process does not allow Federal agencies to keep a "secret" collection of information, to share personal information in an indiscriminate manner, to fail disclosure of the reasons for collecting the information, or to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records.

As I have stressed in my March 14 testimony and in other answers here, the Privacy Office believes this is more than an issue of compliance. Programs that do not clearly define and understand their collection, use, dissemination and maintenance of PII, cannot effectively perform their jobs. In addition, failure to protect PII would imperil the public's support for their efforts.

As such, to the extent that DHS shares information with fusion centers, the fair information principles apply to these exchanges and help determine the controls for the application of any exemptions appropriately taken under the Privacy Act to prevent erosion of privacy protections.

**Question 12.:** Mr. Teufel, your office conducts regular Privacy Impact Assessments to ensure that DHS programs comply with the Privacy Act and other laws.

**As part of any privacy and civil liberties training that your office might offer at fusion centers, how would you go about training fusion center personnel about how to conduct a privacy impact assessment?**

**With adequate resources, would the DHS Privacy Office itself be in a position to conduct Privacy Impact Assessments at fusion centers?**

**Answer:** The Privacy Office has issued Privacy Impact Assessment Guidance, which DHS programs use to draft their own PIAs. Programs must evaluate their collection, use, dissemination, and maintenance of PII, using the eight FIPs.

This guidance would help fusion center leadership and staff to understand the PIA process. In fact, with some slight modifications this guidance is ready for fusion center audiences, since the privacy issues to be examined focus on the FIPs and the collection, use, dissemination, and maintenance of personally identifiable information, rather than the entity doing the PIA. Moreover, since the Privacy Office posts every PIA that is approved on the DHS website, fusion center staff have examples from which to work.

The Privacy Office believes PIAs are most useful to the program when the program staff is heavily engaged in drafting the PIA; with adequate resources, however, the Privacy Office could assist the fusion centers in drafting their PIAs.

**Question 13.: In your view, Mr. Teufel, what is the value of having a Privacy and Civil Liberties Officer within an organization, and how might such an officer have a positive impact at a State or local fusion center?**

**What role could a Privacy and Civil Liberties Officer at a fusion center play in terms of educating the public about the fusion center's purpose and processes?**

**Answer:** The designation of an official with privacy, or privacy and civil liberties responsibilities, within each fusion center is one of the best practices I identified above. As the fusion center guidelines recommend, I believe this Privacy Officer should be in place early in the process of the fusion center's formation. This is the best opportunity to ensure the rest of the recommendations from the fusion center guidelines are implemented. And the fusion center Privacy Officer would be responsible for drafting any PIAs and ensuring that the FIPs are faithfully preserved.

Fusion Center Guideline Number 3 recommends each fusion center have a privacy committee as part of its governance structure. This group would be led by the Privacy Officer. One of the enumerated responsibilities of this committee is to provide outreach activities with the community and interested privacy advocacy groups. I believe this outreach is critical. Public airing of privacy issues is an important step in ensuring transparency, one of the FIPs. Moreover, if the fusion center has implemented all of the FIPs, the Privacy Officer's interaction with the public can help maintain support for their activities.

**Question 14.: Mr. Teufel, there is concern among some privacy advocates about the length of time that information that is not related to an investigation remains in a fusion center database.**

**What are the dangers of not destroying irrelevant information with a prescribed period of time, and how might privacy and civil liberties education at fusion centers address this area of concern?**

**Answer:** Minimalization is the fourth FIP utilized by DHS. This principle includes a prescription that information must be directly relevant and necessary to accomplish the specific purposes of the programs and information must be retained only for as long as it is necessary and relevant to fulfill the specified purpose for its collection. Obviously, fusion centers need relevant information—and only relevant information—to fulfill their mission. Accessing irrelevant and untimely information can only hamper the performance of the hardworking fusion center staff. Such over-collection of information can erode the public's confidence and increase the cost of a security breach with no offsetting benefit to the program.

Privacy training can reinforce the importance of the FIPs. Applying this fourth principle of Minimalization, the fusion center can create criteria for judging the initial relevancy of information and for determining continued relevancy over time. This analysis will aid the fusion center's regular purging of information that, by definition, cannot assist them in performing their important mission.

